UNIVERSITY OF NAIROBI

ASSESSING THE IMPACTS OF SOCIAL MEDIA ON NATIONAL SECURITY IN KENYA

BY

DORCUS PHANICE OLASYA

R52/87706/2016

A RESEARCH PROJECT SUBMITTED IN PARTIAL FULFILLMENT FOR THE AWARD OF A DEGREE OF MASTER OF ARTS IN INTERNATIONAL CONFLICT MANAGEMENT, INSTITUTE OF DIPLOMACY AND INTERNATIONAL STUDIES, UNIVERSITY OF NAIROBI

2018

DECLARATION

This research project is my original work and has not been presented to any other university.

DORCUS PHANICE OLASYA

R52/87706/2016

Signature……………………………………. Date…………………………………

Supervisor

This research project has been submitted for examination with my approval as the University of Nairobi supervisor.

Dr. Patrick Maluki

Institute of Diplomacy and International Studies

University Of Nairobi

Signature……………………………………. Date…………………………………

DEDICATION

This research project is dedicated to my son Ethan Kyle and my family for their love, support both emotional and financial, and encouragement throughout my studies.

ACKNOWLEDGEMENT

I would like to thank Dr. Patrick Maluki, my supervisor for his wise counsel, incisive insight resulting to an immense contribution for this study. I would also like to appreciate my parents Peter and Susan Okemo, who have tirelessly taken care of my son in my absence. To my siblings Jeridah,Ben and Mercy, thank you for your encouragement. Above all, I thank God for His provision, guidance and sustainance, during this period of my training and academic work.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

The usage of social media facilitated by internet boom and emerging mobile technologies has greatly transformed the manner in which the society operates and has also revolutionized the art of communication and sharing of ideas. Through social media platforms such as Facebook, Twitter, Instagram, among others, people from all corners of the world are able to form a virtual home where they interact, communicate and share ideas. While social media has numerous benefits, it does not go without challenges. In the recent past, use of social media has had copious social and security inferences for the citizens, governments and national security agencies including the military and the police. Kenya, being among the countries with the highest social media usage has not been immune to these challenges linked to social media. This study therefore sought to analyse the role of social media on national security with reference to Kenya. Specifically, the study sought to examine the threats of social media usage to Kenya's national security, the use of social media by the security agencies in preventing, limiting or eliminating threats to Kenya's national security, and the various strategies that have been put in place to curb and minimize the negative effects of social media on the national security. The research adopted both descriptive and exploratory research design. The target population comprised of employees of Communications Authority of Kenya. Other key informants included National Cohesion and Integration Commission (NCIC) official, Directorate of Criminal Investigation official, and an official from the National Intelligence Service. Members of the general public were also included in the study. Stratified random sampling technique was used to sample the respondents at the Communications Authority of Kenya. The key informants were sampled through purposive sampling method. The members of the general public were sampled through convenience sampling. Primary data was gathered by use of structured questionnaires and interview guides. Secondary data was gathered from existing records, periodicals, journals, reports, internet sources, policy papers, presented papers and books. Data was then analysed using Statistical Package for Social Sciences (SPSS) using both inferential and descriptive statistics. The findings were presented using frequency tables and figures. From the findings, the study found out that social media is a threat to national security. It was established that terrorist organisations take advantage of social media platforms to facilitate ideological radicalization, recruitment and training, communication, to popularize their actions and to spread propaganda. Social media platforms are also used by community criminal groups to facilitate hate speech, money laundering, among other crimes. The study further found out that security agencies utilize social media to enhance national security mainly through communication with the public, for open source intelligence, for public diplomacy among other purposes meant to enhance national security. The study further concluded that the government has put in place various strategies to minimize the threats of social media to the national security. These include the cybercrime act which offers a framework for timely and effective detection, investigation and prosecution of cybercrimes. The other strategy used to reduce threats of social media on national security is close monitoring of social media groups and content shared online.

CHAPTER ONE
INTRODUCTION

1.1 Background of the Study

Social media usage facilitated by internet boom and emerging mobile technologies is transforming the manner the society operates[1]. The massive technological advancement in the recent past has revolutionized the manner in which people interact and share information. Among the modern improvements is the use of social media platforms. Currently, there is a huge demand for social media by all segments in the society, particularly the youthful generation[2]. Through these sites, people are able to share ideas easily and more effectively and utilize them as key discussion forums. Previously, in the past decades, the only popular communication gadgets were televisions and computers but as a result of technological progress, there are now numerous smaller and portable communication gadgets that have emerged such as wireless laptops, and cellphones which have altered the way people interact and communicate. Through these gadgets, people can virtually link online and share ideas[3].

In the present day, tools of social media have become an essential in the day to day lives of many people across the world. The rate at which Social Media is penetrating into the day to day life is increasing and it is even expected to soar both in the near future and in the long run. This increase has brought with it various effects and has impacted on every aspect of human endeavor from education to health care and many more which are beneficial. On the other hand, social media has various associated demerits that have touched on major areas key among them being national security.

One way in which use of social media has compromised security is facilitation of terrorism. In the modern era, social media platforms are being widely used by terrorist groups for

[1] Tapscott, D. (2009). *Grown up digital* (Vol. 361). New York: McGraw Hill.

[2] Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.

[3] Park, N., & Lee, H. (2012). Social implications of smartphone use: Korean college students' smartphone use and psychological well-being. *Cyberpsychology, Behavior, and Social Networking*, *15*(9), 491-497.

communication, recruitment and training as well as tools for ideological radicalization[4]. In addition, terrorist organisations utilize social networking sites to link up with other criminals such as cybercrime groups and to organize illicit dealings such as kidnappings, drug trafficking and weapon trade. Of late, terrorist organisations which mostly utilize social media to facilitate their operations are the Islamic-jihadists. These groups mostly utilize Facebook and YouTube channels for recruitment and to garner support particularly in the west. All these activities threaten peace and impact on the national security of any particular country. In a similar manner, criminal gangs operating both within and outside a given country utilize social media platforms to garner support, as channels of communication and to coordinate their illegal operations[5].

The other way in which social media can impact on national security is through spread of propaganda. The emergence of social networking sites supplements the use of other media such as televisions, newspapers, and radio to spread propaganda and to influence deception activities all of which disrupts the security of a nation[6]. By the same token, protest movements and revolutionists utilize social media platforms to mobilize the masses. In such a case, these sites are used to better unify, organize and spur masses to action, to arrange demonstrations and to coordinate their tactical and operational aspects. As Gerbaudo [7] argues, through use of social media platforms, the revolutionary groups are able to cut on organization, participation, recruitment and training. As a result, these groups are able to propagate their operations which in turn negatively impacts on national security.

Social media can also impact on national security when the sites are used to diffuse and share confidential, classified or sensitive information or content. While people are granted the freedom of communication and expression, this should not go beyond a point where there is need to safeguard the integrity and confidentiality of classified information so as not to compromise the security of a country.

[4] Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

[5] Patton, D. U., Eschmann, R. D., & Butler, D. A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior*, *29*(5), A54-A59.

[6] Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign affairs*, 28-41.

[7] Gerbaudo, P. (2018). *Tweets and the streets: Social media and contemporary activism*. Pluto Press.

While social media compromise national security in various ways, it also has a number of benefits if properly used by both the public and security agencies. For instance, the government can use social media networking platforms as warning or trend prevention tools. When used as a monitoring tool, the security agencies are able to recognize the first signs of any hostile or possibly precarious activity and they are able to put in place the necessary counter measures. This can be achieved through collection and analysis of messages and other content shared on social media that helps to detect and prevent any occurrences that can threaten national security. The government can also use social media for defence activities such as prevention, warning, prevision, institutional communication, crisis management, and counter-propaganda[8]. In addition, the government can utilize social media an invaluable resource for the collection valuable intelligence since social media subscribers leave traces of their identity, abilities, predilections, movements, contacts, among other details which can be easily gathered and analysed.

A rich theoretical framework underpins this study. One of the theories is the social responsibility theory. According to the proponents of social responsibility theory[9], the media has a key role of serving the public and it should be free from all forms of manipulation for it to achieve this role. According to this theory, there should be well outlined principles in order to make sure that the media fulfills its obligation of keeping the people informed. The theory insists on both the media and the consumers being socially responsible. This therefore implies that if both the media and the consumers become socially responsible, it makes it easier for the government to put in place regulatory frameworks.

Another theory underpinning this study is Technological Determinism Theory. According to the theory, media technologies shape how people in a society think, feel, act and how the society operates as technology evolves. This theory explains the impact of Information Communication Technologies on how information is consumed, retrieved, and disseminated in the modern day society. The theory is premised on the argument that changes in communication modes to a large

[8] Vuori, V., & Väisänen, J. (2009, November). The use of social media in gathering and sharing competitive intelligence. In *9th Internafional Conference on Electronic Business*.

[9] Peterson, T. (1956). The social responsibility theory of the press. *Four theories of the press: The authoritarian, libertarian, social responsibility, and Soviet communist concepts of what the press should be and do*, 73-103.

extent determine the course of history. The theory regards the wider dimension of information craze in the society as a direct result of the information explosion promoted by information and communication Technologies.

1.2. Statement of the Problem

The modern advancement technologies has seen the emergence of better and improved means of communication. This has altered the manner in which people interact and share information across the world. While modern communication technologies particularly the social media has brought numerous benefits, it has also emerged as a growing threat to national security. This is because criminal gangs and terrorist organisations have of late been using social media sites to garner support, and coordinate their operations. Besides being used by terrorist groups and criminal gangs, social media platforms are also utilized by individuals to conduct cybercrimes, and to propagate hate messages and false information to the public regarding state of national security affairs[10]. The perpetrators of such acts in most cases remain at large since they cannot be easily tracked by law enforcement agencies and subsequent prosecution. The security agencies therefore face serious challenges in tracking, monitoring and containing the use and misuse of social media platforms in relation to national security. All these have impacted on national security in various countries across the world.

The negative impacts of social media necessitate strict regulatory measures. It thus crucial to devise a strategy to monitor interactions and communication done via social media networks with an aim of countering adversaries' propaganda and interferences, enhancing state agencies and institutions' performances, as well as reinforcing the geopolitical position of a nation and its international credibility. While these strategies can contribute a lot in the enhancement of national security, adoption and implementation require sophisticated technologies, resources and high expertise which most countries, Kenya included lack. The country, being among the nations which have experienced tremendous growth in the information and communication technologies is not immune to social media forces. It is in this regard that this study sought to analyse the role

[10] Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of communication*, *62*(2), 359-362.

the social media plays on national security. This research also helped to bridge the literature gaps as only a few research studies have been conducted on with reference to Kenya.

1.3 Research Questions

i. What are the impacts of social media on the national security of Kenya?

ii. How can social media be used by security agencies to prevent and limit threats to national security of Kenya?

iii. What strategies have so far been used to minimize negative effects of social media on national security in Kenya?

1.4. Objectives

1.4.1 General Objective

The general objective of the study was to analyze the role of social media on national security with reference to Kenya.

1.4.2 Specific Objectives

The specific objectives of this study are;

i. To examine the impacts of social media usage to national security of Kenya.

ii. To examine the use of social media by the security agencies in preventing, limiting or removing threats to Kenya’s national security.

iii. To examine the various strategies put in place to curb and minimize the negative effects of social media on Kenyan’s national security.

1.5. Justification

The study is valuable to both policy makers and academicians

1.5.1 Policy Justification

It is expected that the findings of this study will give Kenya and other nations insights on how social media impacts on national security. This will inform and guide policies that regulate information sharing through social media platforms. In a similar manner, the study will help to design counter strategy measures on the threats of social media.

1.5.2 Academic Justification

By analyzing the role of social media on national security, the study will contribute to the body of knowledge and form a foundation for other research studies in the same area or in other related topics.

1.6 Literature Review

This section presents a review of literature on the role of social media on national security. The section also discusses the theoretical anchorage of the study.

1.6.1 Theoretical Literature Review

A number of theories can be used to explain the role of media on national security. They include Social responsibility theory and Technological Determinism Theory.

Social Responsibility Theory

The social responsibility theory was articulated in the United States in the early 20th Century on recommendations by the Hutchins Commission on Freedom of the Press. Its major principle was to allow open access to all, with the media being guided by the societal ethical beliefs that form the main environment for exchange of views and opinions[11].The social responsibility theory recognizes the significance of the freedom of speech along with the right to free education, show business and advertisement within a society. The role of the government in this theory is to bring about a favorable environment to the parties involved to reduce the effects of market pressure and trends.

On this theory, Al-Ahmed[12] highlights the major roles of the media as not being limited to serving various political entities but also to enlighten and informs the public. He adds that media needs to assists members of the public by reporting on government administration, improving consumers' education on goods in the market through advertisements and keeping up the media's independence from external and internal pressures.

The social responsibility theory requires the media to not only offer honest and inclusive description of the day to day events in a clear manner, but also be a forum where the public can discuss and criticize especially the government, give a true picture on the representation of the constituent groups in a society and be on the fore front on the presentation and interpretation of the goals and values of the society[13].

It is not only the media reporters and producers who are bound to social responsibility. This extends also to the consumers as they are expected to be media literate and uphold high, yet reasonable expectations of the media. In theory, if both the media and the consumers would become socially responsible, there will be no need for government to intervene through

[11] S. AL-Ahmed, M. (1987). Mass Media and Society: The six Normative Theories and the role of Social, Political and Economic forces in shaping Media Institutions and Content: Saudi Arabia - a Case Study (Ph.D). Leicester University.

[12] S. AL-Ahmed, M. (1987). Mass Media and Society: The six Normative Theories and the role of Social, P olitical and Economic forces in shaping Media Institutions and Content: Saudi Arabia - a Case Study (Ph.D). Leicester University.

[13] Uzuegbunam, C. E. (2013). Social responsibility theory: a contemporary review. A postgraduate Seminar paper presented to the Department of Mass Communication, Faculty of Social Sciences, Nnamdi Azikiwe University Nigeria

regulations. Failure of them to be socially responsible necessitates for preventive measures and regulations. These regulations constitute the very first step in controlling the extent to which media carry out its responsibility towards the public.

The theory of social responsibility is relevant and applicable in the study on the role of social media on national security such that if all the social media users are socially responsible, they will not misuse the available social media platforms in such ways that would compromise the security of a country. Instead, the social media would be used in a manner that contributes to improvement of national security. On the other hand, lack of responsibility would lead to use of social media platforms to spread propaganda, propagate hatred and other deeds that would compromise the national security.

Technological Determinism Theory

This is a reductionist theory that seeks to give the causative linkage between technology and the nature of the society. This theory tries to explain the extent to which human thoughts and actions have been influenced by advancement in technology. According to the theory, the nature of the society is defined by technological advancement and that the course of history is determined by advancement in technology[14].

In modern society, the logics of the media have made a key mark on all fields of social interaction. The social media platforms which have resulted from technological innovation and advancement have brought people closer thus fostering information sharing and exchange of ideas. Technological advancement has led to newer and improved methods of production which has ultimately impacted on the political, economic, and cultural aspects of a society. This has inevitably transformed the society itself[15].

The proponents of technological determinism theory hold that the society is influenced and shaped by technological development and that the society has to adjust and adapt to new and

[14] Qvortrup, L. (2006). Understanding new digital media: Medium theory or complexity theory?. European Journal of Communication, 21(3), 345-356.

[15] Thorsteinsson, G., Page, T., & Niculescu, A. (2010). Using virtual reality for developing design communication. *Studies in Informatics and Control*, *19*(1), 93-106.

emerging innovations and technologies. However, while there have been numerous benefits linked to modern media, there are various negative consequences associated to this advancement due to poor use. According to Toffler, technological advancement is a key determinant of all the changes that have serious effects on all spheres of human life.

1.6.2 Social Media and Social Networking

Social media refers to a group of technologies linked together for rapid information sharing through highly accessible online platforms. The social media platforms that are widely used include blogs, Facebook, Instagram, my space, eBay reputation, Flickr, YouTube, Google maps, Amazon, user reviews, and Twitter. The various social media platforms allow millions of individuals to create online profiles and share personal information with vast networks of friends and, often, unknown numbers of strangers.

Today, unlike the past, there has been a sustained increase in social networking. For instance, currently, Facebook has over 600 million active subscribers with this number expected to increases further while Twitter has over 200 million users globally[16]. Emergence of social media has highly transformed broadcast media monologues into manifold community dialogues, thereby changing the information producer –consumer model into a network whereby each user has the opportunity and capacity to produce and consume internet content.

Social media platforms have well known characteristics. For instance, they enable the users to communicate with each other through various contents such as videos, photos, images, texts and sounds among others. They also help to build and support emerging networks in various fields; whether professionally, family, socially, culturally, religious or politically. Moreover,the social identity of individuals is developed and defined by the previously mentioned platforms.

[16] Statista. (2018). *Number of monthly active Twitter users worldwide from 1st quarter 2010 to 4th quarter 2017 (in millions).* Retrieved April 17, 2018, from Statista: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

They help to develop and define individuals' social identity[17]. As Montagnese[18] argues, social media tools are found to have tremendously higher levels of interaction among its users as compared to traditional media tools which are considered to be having a one way communication flow.

Social media users are considered to be single entities that use media tools to communicate, share information and content, network, improve their personality as well as strengthen their social identity. People use social media platforms to satisfy various needs such as security needs, membership needs, appreciation/esteem needs, and self fulfilment needs. Social networking platforms enable people to pursue their interests, share ideas, and expand their knowledge in faster and better ways than ever before. For social interaction purposes, social media networking sites give users unlimited possibilities online to interact, share collaborate and to correspond to their hearts' content, restricted only by their privacy preferences or security concerns. As a result, social networking is slightly more useful for individuals as compared to organizations and state agencies which are subject to multiple preferences and often more strict security concerns[19].

Apart from using social media for strictly personal purpose, people can also use these networks for the inerests and purposes of the organised groups[20]. Therefore, while social media usage is highly associated with interaction and communication between an individual and the information medium, organized groups including public agencies, states, movements, companies, and terrorist groups are active users of social media networks too[21].

1.6.3 Threats of Social Media to National Security

The security of any country can face threats from social media,which can occur through diverse means. Use of socal media platforms such as facebook, and twitter can cause various negative effects on state security and adverse consequences on the the nation's strategic interests. For istance, widespread use of social networks has increased cases of terrorism in the recenyt past as

[17] Carafano, J. J. (2009). All a twitter: How social networking shaped Iran's election protests. *Heritage Foundation Backgrounder, 2300*.
[18] Montagnese, A. (2012). Impact of social media on national security. *Centro Militare di Studi Strategici (Italy)*.
[19] ibid
[20] Montagnese, A. (2012). Impact of social media on national security. *Centro Militare di Studi Strategici (Italy)*.
[21] ibid

terrorist groups exlpoit these sites to recruit members, and spread their ideologies[22]. Moreover, terrorist groups utilise social media platforms to and cordinate criminal activities, and and to link up with other terrorists cells across the world[23].

To date, the terrorist groups that widely utilise social media platforms to facilitate their operations are the Islamic–jihadists ones. For instance, the Alqaeda widely use Youtube and Facebook to recruit new members and to garner support from sympathisers and supporters across the world. Through the socia media sites, the jihadists are able to spread photos and video footages of successful terrorists attacks in an effort to garners support. Apart from being used as recruitment platforms, the extremists groups utilise the social media platforms to spread propaganda to publicize successful attacks and to spread fear. According to Jones[24], jihadists groups such as the Al-Qaeda developed a well-framed strategy to utilize social media to pursue their goals and to propagate false information and propaganda throughout the world in order to push people to perpetrate terrorist acts.

In a study conducted by Hussaini and Muhammed[25] on the role of social media on national security in Nigeria, the findings indicated that extremist groups widely used social media platforms to perpetrate criminal operations, garner support, spread ideologies and propaganda and to coordinate their operations. This strengthened the organisation hence affecting the state security. The study also established that social media, apart from being used by terrorists and criminal gangs to coordinate their operations, it can also be utilized in various ways to limit and prevent terrorist activities and criminal operations through online monitoring of information sharing and detection of security threats.

In a similar study by Awan[26], the findings indicated that ISIS highly capitalize on online cyber war making use of slick videos, online messages spreading hate and applications meant to

[22] UN Counter-Terrorism Implementation Task Force, (2011), Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary, Riyadh.

[23] Surette, R. (2014). *Media, crime, and criminal justice*. Nelson Education.

[24] Jones S. G., (2011), Awlaki's Death Hits al-Qaeda's Social Media Strategy, RAND Corporation, Santa Monica, CA.

[25] Hussaini, A., & Muhammed, A. (2016). Social Media and The Challenges Of National Security In Nigeria Muhammed. *NUBA Multidisciplinary Journal, 1*(2), 78-89.

[26] Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138-149.

radicalize in addition to creating a new generation of cyber jihadists. Through social media platforms like Facebook, Twitter, and YouTube, the group is able to spread their propaganda and beliefs to numerous online sympathizers across globally.

In a study done in Kenya by Kimutai[27]on the nexus between social media and national security threats, it was established that terrorists use social media for radicalization, spreading ideologies, recruitment, communication and training of its members. The terrorist groups and criminal gangs also use social media to communicate with cyber-criminals and to spread propaganda.

Increase in cyber-crime is a direct consequence of social media, and this has resulted to security breaches of a nation. In the recent past, there have been increased cases of cyber-attacks infiltrating national systems and the ever soaring web of social media sites could prove problematic for national cyber security. As a result of expansion in social media networks, there have been various emerging challenges for government transparency and security.

Cybercrimes occur when people with ill motives use devices, mobile phones and the internet to send messages with the intention of causing embarrassment or hurting other persons in the process. During cyber bullying, the perpetrators conceal their identities behind a computer. This way, the cyber-crime perpetrators are able to act without being recognized. Cyber bullying has also been simplified by the ability to create fake or pseudo profiles. These profiles provide an opportunity to say anything to another individual without the worry of any repercussions. This has facilitated spread of hate speech and incitement which threatens security and wellbeing of the people. Cybercrime perpetration and fuelling of ethical debate has also been facilitated by anonymous blogging. This enables the bloggers to spread information that, if not well monitored can threaten the state security.

1.6.4 The Use of Social Media to Prevent, Limit or Remove Threats to National Security

Social media networks, if properly used by civil institutions and more specifically, by security agencies can represent suitable opportunities to preserve national security. The social sites can also be used by the government for content creation, external collaboration, community building,

[27] Kimutai, J. K. (2014). Social Media and National Security Threats: A Case Study of Kenya. *Unpublished MA Thesis: University of Nairobi*.

and other applications that contribute to enhancement of national security. More importantly, social media platforms can be used at the same time both for defence activities such as prevention, early warnings tools, psychological operations, prevision, strategic communication, open source intelligence (OSI), and counter-propaganda.

Social media networks can be used to promote national security when they are used by security agencies to disseminate information and to foster community policing. The use of social media as well as mobile technology by the public makes it easier to disseminate information, send alert messages, during crises, help in evacuations as well as rescue missions. It also assists in publishing event related information, as well as volunteering and collecting of donations. Apart from being an information distribution tool, social media technologies connect people and information, create and build relationship, establish unofficial networks as well as build communities without boundaries.

Social media networking sites also contributes significantly to national security enhancement. For instance, in the present day, social media can assist during military relief operations. Pillay, Van Niekerk, and Maharaj[28] suggest that security agencies partaking in such activities include social media networking sites into their communication processes so as not only to improve their communication ability but also their ability to coordinate, and share information with other security stakeholders besides the civilian. Through the use of social media, law enforcement agencies across the world are able to take part in the collation, analysis and prediction of intelligence using data gathered from social media networks.

Pandalai[29]in the analysis of the social media challenge to national security established that the Boston Police Department (BPD) made use of social media to disseminate information and to promote community policing in the investigation of the two bomb explosions in 2013 Boston Marathon. In this case, the BPD successfully utilized Twitter to periodically inform the public on the status of the investigation in order to calm nerves and request public assistance, and to correct misreporting.

[28] Van Niekerk, B., & Maharaj, M. (2013). Social media and information conflict. *International Journal of Communication*, *7*, 23.

[29] Pandalai, S. (2016). *The 'Social Media' Challenge To National Security: Impact And Opportunities A Conceptual Overview*. New Delhi: Institute for Defence Studies and Analyses.

Similarly, Pandalai observed that In UK, the Greater Manchester Police utilize online interactive programs that allow the police and the people to interact in an effort to reinforce security. Similarly, the Vancouver police and the Zurich city police, also initiated a programme called ‘tweet-a-thons’ that lasted 24 hours during which the security agencies published all security alerts and activities on twitter in order to enlighten the citizens the broadness of their operations[30].

In India, it was established that police officers preferred using social networking sites mostly to push information or pull information rather than for interaction purposes. The use of online social media proved effective in monitoring and tracking problems, detecting rumors, managing traffic, and in understanding public opinions on various issues[31]. In related findings in the UK, Ghonim[32] established that social media platforms were highly used during the London chaos and protests to fight against rioters and to enhance improve security. In Kenya, Kimutai[33]established that social networking sites are instrumental in dissemination of information and diplomacy gathering by the military in Kenya. These networks give Kenyans a platform to gain access to information and provide feedback on current social, economic and political issues.

Social media platforms have emerged as key channels of information dissemination and have also been instrumental in calling for societal change. In a study conducted by Cragin [34], the findings indicated that social media platforms have emerged as key sources of information and increasingly vital in influencing the people's understanding of terrorism activities and their effects. The widespread use of smartphones has enable people to report suspicious terror activities and to closely follow the aftermaths of terror attacks. For instance in the Paris attack during the Bataclan concert, one of the affected people described the occurrences and pleaded for rescue using social media.

[30] ibid
[31] ibid
[32] Ghonim, W. (2012). *Revolution 2.0: The power of the people is greater than the people in power: A memoir*. houghton Mifflin harcourt.
[33] Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya.* Retrieved April 3, 2018, from UONBI: erepository.uonbi.ac.ke/.../Kimutai_Social%20Media%20And%20National%20Securit...
[34] Cragin, R. K. (2017). The November 2015 Paris Attacks: The Impact of Foreign Fighter Returnees. *Orbis, 61*(2), 212-226.

In a study analysing the role of social media and internet in international relations with specific focus on Arab revolution of 2011 Cuman[35] established that the growth and use of social media in the Arab region played a huge role in mass mobilization of protesters, empowerment, opinion shaping, and influncing change.

1.6.5 Strategies Used To Curb and Minimize The Negative Effects Of Social Media On The National Security

The invention of information technology and its associated communication technologies has proven to be one of the most precious gifts to mankind in the recent past. The epic nature of this technology has had it being rightly termed as the InfoTech revolution. These technologies have fast forwarded the whole human civilization simply by introducing swiftness in information dissemination and communication done via social media[36]. Specifically, social media has greatly transformed political dynamic forces on a global scale by allowing users to express themselves overtly in a manner prohibited before[37]. This way, the social media platforms have decentralized the way people share opinions and information in the society. In addition, it has increased freedom of speech and has enabled access to education.

However, while social media platforms have numerous benefits, it has brought with it various challenges. The very shift in communicative power brought about by the new forms of communication technologies has spawned greater efforts to restrict regulate the usage of social media platforms. This effort of regulating and controlling the use of new forms of communications has led to legal and regulatory initiatives to curb and mitigate risks related to these new communication media, extending from confidentiality of users, intellectual property, national security, to rackets, pornography and hacking.

Currently, governments across the world and the social media companies are at the center of an intense debate on ways that could be used to regulate the social media platforms. The government has a key role of enacting regulation to ensure that the content shared via social media platforms adheres to standards of public decency. The government takes initiatives to take

[35] Cuman K., (2012). The Role of Internet and Social Media in International Relations. Arab revolution of 2011

[36] Aday, S., Henry F., Marc L., and John S. (2010), Blogs and Bullets: New Media in Contentious Politics. Peaceworks, no. 65 (2010). P.11.

[37] Wolfsfeld, G., (2004), Media and the path to peace, Cambridge, Cambridge University Press.

down any offensive content from social media websites when it finds it against the laws of state. Without such regulations, the public and the social media companies cannot take their responsibilities seriously.

The social media companies on their part have a dominant role in what gets communicated in cyberspace and are therefore taking responsibility for their content by barring the spread of propaganda and false information. For instance, Facebook explicitly discourage and bans hate speech. The mission of Facebook is to present opportunities for people to build a close knit community in addition to bringing the world closer together. In order to achieve, this, Facebook removes hate utterances, which takes account of any content that openly attacks populaces based on their color, tribe, national origin, religious affiliation, sexual orientation, sex, gender, or gender identity, as well as serious deformities or diseases.

1.7 Theoretical Framework

The study was anchored on the agenda setting theory[38].

1.7.1 Agenda Setting Theory of the Media

Maxwell McCombs and Donald Shaw propounded the Agenda setting theory in 1970s. The theory implies that exposure to news media leads people in assigning certain significance to various public matters. This is because the media plays a key role in influencing people's perceptions of what is important, acceptable, or desirable. Through the media, attention is drawn to certain aspects of reality and away from others, thereby influencing people in terms of what to think. According to Folarin[39], agenda setting theory is premised on the idea that the mass media predetermines the issues that are considered important in a particular society in a certain time.

Though this theory is popular with the use of traditional media, it is also popular in the current era where modern communication technologies are more and more integrated into the society. Currently, the wide spread use of social media has made the ability to communicate more accessible and convenient. Due to high internet accessibility, people can now communicate their

[38] Peterson, T. (1956). The social responsibility theory of the press. *Four theories of the press: The authoritarian, libertarian, social responsibility, and Soviet communist concepts of what the press should be and do*, 73-103.

[39] Folarin, B. (1998).Theories Of Mass Communication. Ibadan, Nigeria: Sceptre Publishing

ideas and opinions to a wider audience within a short duration of time. Due to the widespread use of social media, its adverse effects can now be felt, one of the areas affected being the national security. For instance, terrorist organizations utilize the social media to divert people's attention to their operations. Through, this, they are able to popularize their ideologies and to garner support. Apart from the terrorist groups, other organized gangs utilize the social media networks to popularize their activities and to coordinate their operations. The rationale for adopting the Agenda Setting Theory in this study was because it explains the function of the social media in molding and shaping people's opinions on some topical issues in this case national security.

1.8. Hypotheses

The study tested the following hypotheses;

1. Uncontrolled use of social media by the public can significantly compromise Kenya's national security.
2. If social media is well utilized by security agencies, it can greatly help to prevent and limit threats to Kenya's national security.

1.9. Methodology

The section discusses the methodology applied in data collection and its subsequent analysis. The key issues discussed here included the research design, the target population, the sample size determination, data collection tools and procedures, and data analysis.

1.9.1 Research Design

Descriptive and exploratory research designs were utilized in this study. The descriptive design provided a picture of current situation in regards to the role of social media on national security. The exploratory research design on the other hand was used to carry out an in-depth analysis of the link between use of social media and national security. Exploratory design is comparatively easy to understand and to explain. In addition, it is easy to use data collected using exploratory design to suggest likely reasons and to give conceptual models of these relationships.

1.9.2 Target Population

The target population is the complete set of items or a group of people from which the researcher wishes to obtain data[40]. In this study, the target population comprised of the general public, employees at Communications Authority of Kenya, National Cohesion and Integration Commission (NCIC) official, Directorate of Criminal Investigation official, and an official from the National Intelligence Service. The governments bodies chosen to partake in the study are involved in matters of state security are therefore considered to be well placed to give data for the study. Inclusion of the general public was also crucial since they are the highest users of social media platforms.

1.9.3 Sampling frame/Sample size

Participants of interest were employees of Communication Authority of Kenya. According to the records, there are 500 employees at the communication authority of Kenya[41]. The sample was therefore be computed using the Yamane's formula as follows;

$$N = \frac{N}{1 + Ne^2}$$

$$N = \frac{500}{1 + 500(0.1^2)}$$

$$N = 83 \text{ Employees}$$

The study used a sample size of 83 employees. In a descriptive study, a sample size of 10-50% is sufficient to yield reliable findings[42]. Therefore, a sample of 83 employees was a good representation of the target population. The researcher used stratified random sampling technique to sample the respondents. Stratification was done to ensure the various departments at the communication authority of Kenya are included in the study. Simple random sampling was used to pick the respondents from each department. This method gave all the staff members equal

[40] Mugenda, O. M., &Mugenda, A. G. (2003). Research Methods: Quantitative And Qualitative Approaches. Nairobi: Acts Press.

[41] Crunbase. (2018). *Communications Authority of Kenya.* Retrieved May 28, 2018, from Crunch base: https://www.crunchbase.com/organization/communications-authority-of-kenya

[42] Mugenda & Mugenda (2003) Research Methods: Acts Press, Nairobi.

chances of being included in the sample[43]. The key informants including the National Cohesion and Integration Commission (NCIC) official, Directorate of Criminal Investigation official, and an official from the National Intelligence Service was sampled through purposive sampling as they are deemed to be well acquainted on matters of national security. Members of the general public will be sampled through convenience sampling.

[43] Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International

Table 1.1: Sample Frame

Department	Sample Size
Communication Infrastructure	20
Regulation and Access	20
Operations Team	20
Legal and enforcement Team	20
Total	**80**

Source: Crunbase. (2018)

1.9.4 Data Collection Tools and Procedures

To achieve the objectives of this study, both primary and secondary data were used. Primary data was gathered from the employees of Communication Authority of Kenya and key informants from the National Cohesion and Integration Commission (NCIC), Directorate of Criminal Investigation, and the National Intelligence Service by use of structured questionnaires. The questionnaire was sectioned differently according to the objectives to make it easier for the participants to fill. The public opinions were collected using structured data collection schedules. Secondary data was gathered from existing records at the National Cohesion and Integration Commission, periodicals, journals, reports, internet sources, policy papers, presented papers and books. These sources provided insight on what is already known about the problem of the role of social media on national security.

1.9.5 Validity and Reliability of the Research Instruments

Validity test is an analysis that helps the researcher to assess the accuracy of the research tools and the truth of the results obtained. In this study, both content and face validity were used. Content validity involved consultations with the supervisors and research experts. Face validity involved checking for clarity of the questions in an effort to enhance the research instruments. On the other hand, a research tool is said to be reliable if it yields consistent results over a period of time. Test-retest reliability method was used to determine the consistency of the questionnaires administered. To achieve this, a Cronbach coefficient alpha statistic with a cut-off point of 0.6 was used. According to Best & Kahn[44], a reliability coefficient of 0.6 and above is sufficient for an instrument to be considered reliable.

1.9.6 Data Analysis

The completed questionnaires were scrutinized carefully to ensure completeness and consistencies. Data was then analysed using Statistical Package for Social Sciences (SPSS) using descriptive methods. This involved means, standard deviations, and percentages. The findings were presented using frequency tables and figures.

1.9.7 Ethical Concerns

Ethics are important in research because they spell norms that guide any research activity, particularly the way researchers will gain authorization to collect data and the behavior expected from them in the field. Accordingly, the researcher acquired clearance letters from National Commission for Science, Technology & Innovation (NACOSTI) as well as the University of Nairobi. During the process of data collection, informed consent was the mainstream criteria of each respondent participating in the study. In addition, the researcher ensured that the respondents and the organisation are protected by keeping their identity and all the information gathered confidential.

1.10. Chapter Outline

This research report is structured as follows:

Chapter one discusses the background of the study, statement of the problem, research objectives, and significance of the study, the literature review, theoretical framework, the research methodology and the chapter outline.

Chapter two examines the threats of social media usage to Kenya’s national security. Chapter three discusses the use of social media by the security agencies in preventing, limiting or removing threats to Kenya’s national security.

[44] Best, J.W. and Kahn J.V. (2006) Research in education. United States of America: Pearson.

Chapter Four examines the various strategies that have been put in place to curb as well as minimize the negative effects of social media on the national security.

Chapter five provides the summary of the findings, conclusions and the recommendations.

CHAPTER TWO

THREATS OF SOCIAL MEDIA USAGE TO NATIONAL SECURITY

2.1 Introduction

This chapter discusses the threats of social media usage on national security. It discusses the various ways in which use of social media platforms compromise the security of individuals, organisations and state security. In addition, various cases have been cited where social media platforms lead to security breach.

2.2 Social Media Usage and National security

Social media platforms are web based services in which people build profiles within a bounded system and through which they create connections with other users across the globe. Social networking involves creation of relations among people who have common interests and goals. Lately, social media platforms such as Facebook, Twitter, YouTube, LinkedIn, Skype, 9jabook, Lagbook and among others have solidified their positions in the hearts of many users across the world, what has made hackers and other people to utilize them to achieve their malicious aims[45].

In the recent past, events across the world have indicated that the use of social media, just like other traditional media can threaten the security of a nation. It is worth noting that the security of any particular nation is of key importance in the maintenance of peace and harmony[46]. In the recent past, countries across the world have been facing a myriad of security challenges with one of the fueling factors being misuse of social media platforms. It is worth noting that the social media networks are not security threats in themselves but it’s the subscribers of these platforms who pose security challenges through their anti-social endeavors. This is particularly the case when there is limited government oversight, less incentives to inform and educate the users on information security, limited knowledge on online privacy, and lack of knowledge in how the

[45] Coiera, E. (2013). Social networks, social media, and social diseases. *BMJ: British Medical Journal (Online), 346*.

[46] Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

misuse of these platforms can compromise the national security[47]. This implies that, while social media has numerous benefits to both an individual and the nation in general, it can lead to destabilization of a nation among other well-known security risks to a nation[48]. For instance, usage of social sites by people may lead to violence and conflict through sustained messages of hatred and propaganda. Therefore, debates surrounding the use of different social networking platforms should center on the bigger discussion regarding national security and information flows.

There have been numerous cases reported involving use of social networking sites by criminals to spread malicious cryptogram to compromise the users computers or to gain access to personal information such as location, contact details, and professional relationships. According to a survey conducted by Sophos in 2009, Facebook is the most vulnerable social media platform to cybercrimes. Cyber criminals utilize this site together with other social media platforms to disturb security trough spread of viruses, spread of third party applications, to perpetrate social engineering attacks, to carry out identity theft, among other threats[49].

2.2.1 Social Media and Terrorism

Social media has emerged as one of the key tools used by terrorist cells and organisations to facilitate their operations. Currently, with the widespread of modern information and communication technologies, cyber terrorism has emerged as a key compromise to the security of nations across the world[50].

Today terrorist choose social media networks as a practical alternative to destabilize disturb individuals, organisations and to destabilize national peace. At the same time, based on the affordability, convenience and extensive coverage of social media networks particularly

[47] Sykora, M. D., Jackson, T. W., O'Brien, A., & Elayan, S. (2013). National security and social media monitoring: A presentation of the emotive and related systems. In *Intelligence and Security Informatics Conference (EISIC), 2013 European* (pp. 172-175). IEEE.

[48] Wanner, G. (2011). Risks of social media to organizations: Oaks publishers UK. P 64

[49] Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2014). Privacy and national security issues in social networks: the challenges. *arXiv preprint arXiv:1402.3301*.

[50] Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global.

Facebook, YouTube, and Twitter, terrorists have to a large extent utilized these platforms to promote their ideologies and to garner following across the world.[51]

The social networks are currently being utilized by the groups to design and coordinate attacks, to link with other affiliated terrorist cells and criminal groups, to spread false information and propaganda, and to propagate hate that can injure the sentiments of the public[52]. The terrorist organisations now have their own websites which enables them to spread their ideologies and propaganda and they also have various social media channels through which they link up to champion their ideologies. Currently, the social media chat services such as Skype which has both audio and visual capabilities has become very popular among the various terrorist organisations. Through chatrooms and e-forums, the insurgents are able to interact and communicate with each other and with their sympathizers from all over the world. This also enables them to recruit new members and to share information with minimal or no risks of identification by the security agencies.

In the modern era characterized by online connectivity and widespread use of social media networks, terrorists are highly using the platforms for radicalization, recruitment and to train new recruits new members across the word[53]. According to Lorraine Bowman-Grieve[54], social media platforms play a key role in influencing individuals to partake in collective actions. They facilitate social contacts and social bonding which in turn manipulates behavior and attitudes over time. As a result of considerable publicity of extremist ideologies and materials, vulnerable individuals may be compelled to join the jihadist groups. Besides the above mentioned ways in which the insurgents use social media platforms, these groups utilize social networks to coordinate with other criminal gangs and to seek funding from various sympathizers across the world. With great technological advancement, the use of social media has considerably

[51] Freeman, L., Schroeder, R., & Everton, S. F. (2017). Social Media Exploitation by Covert Networks: A Case Study of ISIS. *Communications of the Association for Information Systems*, *41*(1), 5.

[52] Tsesis, A. (2017). Social Media Accountability for Terrorist Propaganda. *Fordham L. Rev.*, *86*, 605.

[53] Lara-Cabrera, R., Pardo, A. G., Benouaret, K., Faci, N., Benslimane, D., & Camacho, D. (2017). Measuring the radicalisation risk in social networks. *IEEE Access*, *5*, 10892-10900.

[54] Bowman-Grieve L., (2010). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment, Euro ISI Conference Submission, Leeds.

facilitated the linkage between the terrorist groups and organized crime and this has facilitated the production of new offensive technologies[55].

Currently, the terrorist cells and organisations that highly utilize social media platforms are the Islamic-jihadist groups. The net-like decentralized structure of most of these groups enable them to utilize social media networks such as Facebook and twitter to effectively link all the groups affiliated to them and to coordinate their leadership across the world[56]. The al-Qaida for instance utilize the social medial platforms mainly to coordinate its leaders, to recruit and train their members, to garner support from all over the world, to seek funding, to publicize their successful operations through pictures and videos, to publicize a list of their martyrs, and to propagate their ideologies. Other groups such as the ISIS and the alshabab use the social media not only for recruitment and training but also to promote their ideologies, to publicize their successful operations, and to spread fear among the civil population.

Social media platforms are also highly misused by the jihadist groups to spread fear and panic among the public. According to The US Congressional Research Service[57], some terrorist organisations and organized criminal gangs utilize the social media networks to spread false information during catastrophic occurrences such as floods, earthquakes, and nuclear blasts with an aim of overdrawing their damaging aftermaths in order to mystify the people and to delay response actions and emergency operations. They also use the online platforms to spread pornographic content, virtual identity theft, phishing, and spread of malware, to co-ordinate arm trade and drug trafficking, to promote human trafficking, money laundering, among other illegal activities[58]. All these compromise and worsen the security of the affected nation.

[55] Blitzblau S., (2011). Analisitecnicadellecapacità di NetINTdeigruppiterroristici, Information Warfare Conference 2010, Franco Angeli, Milano.

[56] Rollins J., (2011), Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy, Congressional Research Service, Washington, DC.

[57] Rollins J., (2011), Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy, Congressional Research Service, Washington, DC.

[58] Intelligence And National Security Alliance, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA.

2.2.2 Social Media and Spread of Propaganda

Propaganda refers to a form of communication especially of a misleading and biased nature which is meant to publicize or champion a specific point of view. According to Snow[59], propaganda is a form of persuasion aided by controlled transmission of single-sided information via the media especially the social media platforms. According to the report by the World Economic Forum in its Global Risks, the rapid spread of deceitful and fabricated information via social medial networks is one of the key emerging threats. Unlike in the past where communication and information sharing occurred through traditional media, currently, the extensive growth of the internet has revolutionized the art of information sharing an aspect propagandist has taken advantage of[60].

The internet is a wilderness of information which unlike the traditional media are almost impossible to monitor and regulate. Due to stringent social media regulatory frameworks, terrorist groups, criminal gangs, and ill-intentioned individuals are currently taking advantage of the convenience and extensive coverage of social networks to spread propaganda and this has emerged as one of the key threats to national security across the world[61]. The al Qaeda group for instance has a well framed strategy that utilizes social media platforms to propagate propaganda to their members across the world in order to persuade them to perpetrate criminal activities [62].

The group also utilizes social media networking sites to spread fear through news bulletins, broadcasts of grotesque images of beheadings among a series of other horrifying incidents. A good instance of this is the case whereby the Syrian extremist group known as the Islamic State of Iraq and Syria (ISIS) went live on social media to show an act in which they severed a man's hand[63].

[59] *Snow, N(2008). Routledge Handbook of Public Diplomacy. p. 338*

[60] Abrahms, M., Beauchamp, N., & Mroszczyk, J. (2017). What terrorist leaders want: A content analysis of terrorist propaganda videos. *Studies in Conflict & Terrorism*, *40*(11), 899-916.

[61] Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

[62] J0nes. G., (2011), Awlaki’s Death Hits al-Qaeda’s Social Media Strategy, RAND Corporation, Santa Monica, CA.

[63] Wood, G. (2015). What ISIS really wants. *The Atlantic*, *315*(2), 78-94.

2.2.3 Social Media and Revolutionary Activities

The speed at which information is spread via social media platforms is the key reason why various platforms such as Facebook and Twitter ply a large role in civil society even fueling revolution. In the Libyan revolution, social media platforms were highly used to distribute information and to provide coverage of the occurrences within the country. Since the mainstream media platforms were controlled by the state, social media networks became the reliable sources of information for the masses involved in the revolutionaries[64]. During the demonstrations, YouTube was highly used to show the happenings on the streets and as a result, social media and mobile tools such as cellphones and tablets were crucial in the revolution as they helped to garner more supporters which ultimately compromised and worsened the security of the nation.

Another instance where social medial platforms were utilized to facilitate revolutions is the Arab Spring. In this occurrence, the world was thrown into chaos via tweets, YouTube videos, and numerous posts on Facebook and blogs[65] by the masses who wanted their voices to be heard. In this instance, the revolution started in Egypt and within a short duration, it had spread across Northern Africa and across the Middle East.

2.2.4 Social Media and Information Leaking

Information leakage refers to a breach of the privacy of information which usually leads to disclosure of vital confidential information into the public domain[66]. This is in most cases caused by malicious and non-malicious individuals who in most cases have access to the information[67]. Extensive empirical evidence has shown that vital information can easily be leaked through the social media platforms, face to face interactions, through print material, through emails, via cloud computing, domain name systems, and via portable data devices. Of all these, social media networks have been identified as the most challenging channel through which information can be

[64] KimGarst. (2018). *4 Instances When Social Media Fueled a Revolution.* Retrieved May 16, 2018, from Kim Garst: https://kimgarst.com/4-instances-when-social-media-fueled-a-revolution

[65] KimGarst. (2018). *4 Instances When Social Media Fueled a Revolution.* Retrieved May 16, 2018, from Kim Garst: https://kimgarst.com/4-instances-when-social-media-fueled-a-revolution

[66] ISO/IEC (2005). Information technology - Security techniques - Code of practice for information security management, ISO/IEC 17799:2005(E)

[67] CSI. (2009). 14th Annual CSI Computer Crime and Security Survey: Executive Summary. New York: Computer Security Institute.

leaked because information leaked via social media platforms gives cyber criminals a chance and a good avenue to gather intelligence , to sabotage organisation's networks through malware attacks, and to use resources to launch the applications on these networks[68].

While information leakage can occur via offline social interactions platforms such as meetings, conferences and publications, the leakage via online social networking sites is fundamentally different from the offline counterparts. This is because when sensitive information is leaked online, the published information almost permanent, which makes it available to many people, and possibly be copied and spread to other people thus extending its reach. Unlike in social media, in case of information leakage via the word of mouth during conversations, the leaked information is confined to the people who heard it and it losses validity if communicated to other people since it can be perceived as hearsay and untrue. This therefore limits the ability of the information to be spread widely[69].

Typical social media platforms have the functionalities such as status updates, friends' requests, photos and videos uploads, third party applications and links to other websites which makes them likely avenues through which information can be leaked. In addition to this, social media platforms just like other web 2.0 applications enables the user profiles to be leaked by other people. It makes it possible for other users to access and copy the information, to alter the information and possibly to distribute it to other people[70].

Social media networks have lately been on the spotlight linked to numerous cases of breaching the privacy of their users. There have been cases whereby social media compromises the security of a nation when classified information is leaked. Currently, with the extensive use of social media platforms, there have increased cases of non-authorized and uncontrolled publication of classified and sensitive information through social media networks. In such cases, the national security is severely compromised.

[68] Gudaitis, T. (2010). The Impact of Social Media on Corporate Security: What Every Company Needs to Know: Cyveillance, Inc.

[69] Jansen, J. (2010). Strategic information disclosure and competition for an omperfictly protected innovation. The Journal of Industrial Economics, 58(2), 349-372.

[70] Jacobsson, S. (2010). Social Networks May Be Sharing Your Info with Advertisers. PC World.

Irresponsible use of social media networks causes detrimental effects in terms of putting organisation's systems and networks at risk of malware attacks which results to law suits as a result of defamation and copyright, loss of data and information, loss of productivity and significantly affecting the reputation of the organisation and its future prospects. A good example where social media compromised the security of a nation occurred in Israel whereby one of the Israeli military officials revealed the time and location of a planned operation via his Facebook status update which led to the cancellation of the operation[71].

Another instance of vulnerability of confidential information to misuse is the availability of Facebook accounts in torrent sites that can be downloaded, what exposes the information of over 170 million Facebook subscribers across the world[72]. Another instance where misuse of social media platforms compromised security occurred in the UK where the employees in the ministry of defense exposed the country's security secrets to the people public through twitter and Facebook networks[73.] Another similar case occurred in India involving four Indian senior naval officials who were accused of disclosing classified information about the location of warships, armaments, and patrolling patterns[74].

2.2.5 Social Media and Financial Fraud

Social media platforms are utilized for electronic financial fraud and hacking. Cyber criminals use malware to steal vital banking credentials and to wire out money. Hackers also utilize ransom ware to hold users accounts hostage and later demand for cash. A good instance of this is the a Facebook targeted malware dubbed Carberb that is hidden in PDF and Excel files that get activated once opened and they harvest vital credentials for social networking sites and emails.

[71] BBC. (2010). Israeli military 'unfriends' soldier after Facebook leak. Retrieved 9 March 2010, from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

[72] Paul, I. (2010). The Facebook data torrent debacle: Q&A. PCWorld.

[73] Mansfield, R. (2010). UK MoD Secrets Leaked Onto The Internet. Retrieved January 25, 2010, from http://news.sky.com/skynews/Home/UK-News/Ministry-of-Defence-Staff-Have-Leaked-Secret-Information-16-TimesOnto-Social-Networking-Sites/Article/201001415535304

[74] Moskos, C. "The Media and the Military in Peace and Humanitarian Operations." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago.

This virus not only collects user information but it also holds user accounts hostage and demand for ransom[75].

Another virus that is mostly spread via Facebook is known as Ramnit. This virus is particularly threatening to enterprises and it mostly steals Facebook login credentials and enables the perpetrator to perform various remote control exploits. Another malware that utilized just like Carberb to perpetrate financial crimes is known as Spy Eye Trojan. This virus has the capability to gain access to bank accounts of the victims by use of the stolen credentials[76]. This Trojan not only has the ability to withdraw cash but it also hides the transactions to the account holder such that it always intercepts the account owners attempts to retrieve balance information and instead replaces the fraudulent activities with the owners past transactions such that the account holder becomes aware of the fraud when the bank refuses to authorize transactions or when the account owner gets a printed statement of all the transactions from the bank[77].

In Kenya, currently, it has become very common for financial institutions in Kenya and across the world to experience huge financial loses annually via online technologies. Currently, the new technologies have made banks and other financial institutions more vulnerable to numerous threats such as phishing, identity theft, card skimming, viruses, and Trojans, spyware, and adware, social engineering, website cloning, and cyber stalking. In 2011 for instance, the Kenya's central bank anti-fraud unit reported that the country's financial sector suffered a loss of over Kshs. 1 billion through electronic financial fraud[78]. This form of fraud became so common that in general, in 2011, about 105 big organisations both in the private and public sectors including the Communication Commission of Kenya (CCK) were hacked. All these were major threats to the national security.

[75] Leyden, J. (2012). *New stealthy botnet Trojan holds Facebook users hostage.* Retrieved August 8, 2018, from The Register: https://www.theregister.co.uk/2012/01/18/carberp_steals_e_cash_facebook/

[76] Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware. In *Global Security, Safety and Sustainability & e-Democracy* (pp. 204-211). Springer, Berlin, Heidelberg.

[77] Etaher, N., & Weir, G. (2014, June). Understanding the threat of banking malware. In *Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics* (pp. 73-80).

[78] Panayiotides, N. (2015). The Islamic State and the redistribution of power in the Middle East. *International Journal on World Peace, 32*(3), 11.

Increased use of the internet and social media platform has also led to high cases of cyber laundering. This occurs when cyber criminals take advantage of the online platforms to convert criminal financial dealings to untraceable funds[79]. Here, cyber criminals do not channel funds directly to their accounts but instead utilize indirect channels through money mules[80]. Money mules are the individuals engaged by the cybercriminals to receive the money received fraudulently and they later fraudulently channel the money to the fraudsters.

2.2.6 Social Media and Spread of Malware

Easy accessibility and extensive reach use of social media platforms have made them suitable avenues for malicious attacks. People on social media share a lot of seemingly innocuous information that is exactly the type of information that hackers and cyber criminals like to gather and utilize in their phishing and spear phishing campaigns[81]. The cyber criminals on the other end are continually perfecting their ability to stalk social media users and infect them with their malware. Since social media networks such as Facebook and Twitter have a very wide audience, the criminals are able to infect a large number of users.

As the world becomes increasing interlinked through the internet and other communication technologies, cases of information security breach have increased considerably in the recent past. Regardless the threat of malware and viruses being there did not gain traction until the emergence of the internet and its extensive use which have given hackers and cyber criminals an avenue to test and sharpen their skills. As a result, there have been increased cases of cyber criminals compromising websites, stealing data, or engaging in fraudulence. All these compromise security of the organisations affected the general public and national security.

In the modern era, there are numerous cases of malware attacks due to widespread use of the internet and social media platforms. Cyber criminals are currently taking advantage of social

[79] Leslie, D. A. (2014). Cyberlaundering: Concept & Practice. In *Legal Principles for Combatting Cyberlaundering* (pp. 55-117). Springer, Cham.

[80] Leukfeldt, R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology*, *9*(2), 173.

[81] Molok, N. N. A., Ahmad, A., & Chang, S. (2011). Information leakage through online social networking: Opening the doorway for advanced persistence threats. *Journal of the Australian Institute of Professional Intelligence Officers*, *19*(2), 38.

media platforms to spread computer viruses and malware whereby attackers use specialized techniques to gain unauthorized access to other user's accounts to compromise them[82]. Hackers create malware for varied aims key among being the desire to cripple the government or for personal benefits. Some of these attacks are meant to harm the systems in which they are installed, some are meant to take over the systems in which they are installed in order to attack third parties, while others are not meant to cause damage but to help the perpetrators to steal data from the specific system[83]. All these, particularly those directed to government agencies cause serious threats to the security of the state.

One of the remarkable instances in which social media compromised security through malware attacks occurred in 2005 when MySpace subscriber developed a warm which enabled him to add a million entries into his contact list. This worm launched a script to users searching for exploitable vulnerabilities to perpetrate malicious acts such as infecting cookies with malware, opening SSL connections among other acts[84]. A similar instance which caused serious effects occurred in 2006 whereby a worm was created and spread through the profiles of MySpace users. In this instance, the malware created infected every user who visited a certain profile[85].

Another social media malware attack occurred in 2007 involving Facebook. In this instance which took place in Illinois (USA), a man disguised himself as an adolescent to attract children and to share malicious photos with them. This man was however arrested and Facebook was highly criticized for failure to protect children[86]. Another serious instance of malicious attack via social media platforms occurred in December 2007 when a Canadian porn company hacked more than 200,000 users' accounts, and gained access to data which included user names,

[82] ibid

[83] Scherer, M. (2011, May 30). Can They Win, One Tweet at a Time? , Time. State of California, Office of the State Chief Information Officer

[84] Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

[85] Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

[86] Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cyber crime and security. *International Journal of Research in Engineering and Applied Sciences*, *2*(1), 48-51.

passwords, and email addresses[87]. This seriously compromised the information security of the social media users.

In yet another instance, Russian operatives used LinkedIn phishing to distribute malware to various institutions and government bodies in the United States of America. In this attack, the Russians used fake Harvard email address in an attempt to spread malware into the American government bodies and various non-profit organisations[88]. In this attack that occurred immediately after the US general elections, the attackers created a PDF document dubbed “Why American Elections Are Flawed.” and inserted malware into it. Using a fake email address similar to that of Harvard lured the people to open the email thus spreading the malware[89]. This is an indication that it is very easy for cybercriminal to use and manipulate the exact domain names of organisations that are not protected by email authentication.

Another malware involved the parliament of Japan. In this attack, the Japanese parliament suffered a Trojan attack that had its origin in China[90]. The computers and servers in the lower house of the Japanese parliament became infected by viruses when one of the members opened an email attachment[91]. It was later revealed that the cyber attackers who perpetrated this crime were able to gain access to key passwords and other data on the infected computers. Another country that has recently suffered malware attacks is Taiwan with most of the attacks originating from China[92]. There have been multiple hacking attempts which mostly aimed at stealing vital and classified government data and information. In most of these cases, the cyber criminals used Taiwan as a proving ground in their efforts to refine their cyber espionage skills.

[87] Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cyber-crime and security. *International Journal of Research in Engineering and Applied Sciences*, *2*(1), 48-51.

[88] Garcia, A. (2016). *How the Russians hacked into U.S. institutions using a fake Harvard email address.* Retrieved August 8, 2018, from Linkedin: https://www.linkedin.com/pulse/how-russians-hacked-us-institutions-using-fake-email-garcia-tobar

[89] Garcia, A. (2016). *How the Russians hacked into U.S. institutions using a fake Harvard email address.* Retrieved August 8, 2018, from Linkedin: https://www.linkedin.com/pulse/how-russians-hacked-us-institutions-using-fake-email-garcia-tobar

[90] Russell, J. (2011). *Japanese government hit by Chinese Trojan horse attack.* Retrieved August 8, 2018, from henextweb: https://thenextweb.com/asia/2011/10/25/japanese-government-hit-by-chinese-trojan-horse-attack/

[91] Russell, J. (2011). *Japanese government hit by Chinese Trojan horse attack.* Retrieved August 8, 2018, from henextweb: https://thenextweb.com/asia/2011/10/25/japanese-government-hit-by-chinese-trojan-horse-attack/

[92] White, E. (2018). *Taiwan hit by jump in cyber attacks from China.* Retrieved August 8, 2018, from Financial Times: https://www.ft.com/content/8e5b26c0-75c5-11e8-a8c4-408cfba4327c

China has also suffered a series of cyber-attacks. In one of the greatest cyber-attacks that occurred in 2013, the internet services were taken down by a powerful malware attack which was believed to have originated from very skilled perpetrators[93]. This was the worst of all the cybercrimes the country had suffered in history[94]. The United Kingdom is yet another country that has suffered a series of malware attacks. On May 2017, the UK was among the countries that were hit by a ransom ware dubbed 'WannaCry' that was spread by a group of cyber criminals called Shadow Brokers[95] . In this instance, the malware used infected hundreds and thousands of public utilities and large corporations. Some of the worst hit sectors included the country's National Health Service hospitals and facilities[96] .

Barely two months after the Wannacry ransom ware, another series of ransom were infections spread all over the world. This malware dubbed Petya was a bit more advanced than the Wannacry and managed infect a large number of key government systems and some organisations[97]. Among the worst affected organisations included the US pharmaceutical company Merck, Danish shipping company Maersk, and Russian oil giant Rosnof.

2.2.7 Social Media and Social Engineering

In the recent years, social media platforms have become a hotbed for cybercriminal activities. Of late, social engineering has emerged as one of threats to individuals, organisations and the national security at large. Social engineering refers to a process whereby cyber criminals psychologically manipulate an unsuspecting individual into revealing confidential details and information through various methods such as identity theft, spam, and phishing. These compromises the information security be it of an individual or an organisation. It is worth noting that it is crucial to uphold information security particularly because, failure to do so can lead to

[93] Paganini, P. (2013). *China hit by DDoS attack. The Internet inaccessible for hours.* Retrieved August 8, 2018, from security affairs: https://securityaffairs.co/wordpress/17327/cyber-crime/chinas-hit-ddos-attack.html

[94] Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

[95] Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

[96] Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

[97] Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

serious security breach which can adversely impact on the organisation or the individual affected. This is particularly the case nowadays where the threat of terrorism is highly looming in the background[98].

Social engineering occurs in various forms. In some case, the perpetrator directly contacts the victim and tries to solicit personal details through the phone and via social media platforms. In other cases, the attackers contact a third party such as executive assistants, office administrators, and IT staff to solicit for classified information. Perpetrators utilize this method to ask for personal information such as birthdates. In other cases, cyber criminals utilize this method together with other methods to attack and breach organisations and gather data. This compromises the national security[99].

Criminals have utilized social engineering over a long duration to exploit human behavior and to bypass complex and secure infrastructure and systems. According to a security industry survey, social engineering is among the most common hacking methods. Cyber criminals and intruders are revolutionizing the various ways in which they can gain access to valuable resources including the information systems of organisations as well as personal information that they can utilize for malicious purposes and for their personal benefit. More recently, cybercrime perpetrators have been taking advantage of people's desire for news and social relevance to socially coerce people to disclose classified information. All these compromise the security of the individuals and the nation in general[100]. There are various documented cases whereby social engineering led to devastating losses. For instance, in 2002, increased cases of cybercrimes particularly social engineering cost organisations in the US huge sums of money amounting to $266 million[101]. In a study conducted by the San Francisco-based Computer Security Institute (CSI) and the San Francisco FBI, the findings indicated that approximately 90% of 273 participants detected some form of security breach in through social engineering in 2002.

[98] Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Reading Room*.

[99] Hinkley, C. (2011). *Social Media Makes Way for Social Engineering.* Retrieved May 18, 2018, from Security Week: https://www.securityweek.com/social-media-makes-way-social-engineering

[100] Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Reading Room*.

[101] ibid

CHAPTER THREE

THE USE OF SOCIAL MEDIA BY THE SECURITY AGENCIES IN PREVENTING, LIMITING AND REMOVING THREATS TO NATIONAL SECURITY

3.1 Introduction

Social media allow for extensive connections and widespread sharing of information. As a result of their wide reach, terrorists and other criminal cells have exploited them to disturb security of individuals, organisations, and the general security of a nation[102]. For instance, terrorist organisations make use of social media platforms to conduct recruitment, to garner support from all corners of the globe, to popularize their ideologies, to publicize their operations among other motives[103]. Social media platforms are also widely used to perpetrate cybercrimes, to conduct malware attacks, as well as to coordinate other illicit deals. All these have impacted negatively on the public security.

While it has been seen that social, media networks can negatively demoralize national security in myriad ways, however, they can also represent an effective opportunity to protect and preserve national security[104]. If well utilized especially by the state security agencies, social media platforms have the potential of reaching the strategic interests of a nation and to preserve national security. For instance, governments can use social media tools for content creation, community building and for international collaboration among other applications. In addition, social media tools can also be used both for defence activities such as prevention of terrorist activities, early warning detection, strategic communication, as a source of intelligence, psychological operations, counter-propaganda among other use. In this regard, it can be argued that it is crucial for security agencies to progressively refine and update plans in a bid to disrupt the emerging internet technologies that are likely to compromise the state security[105]. Failure to

[102] Kumar, G., & Kumar, K. (2014). Network security–an updated perspective. *Systems Science & Control Engineering: An Open Access Journal*, *2*(1), 325-334.

[103] Nacos, B. (2016). *Mass-mediated terrorism: Mainstream and digital media in terrorism and counterterrorism*. Rowman & Littlefield.

[104] Kilcullen, D. (2006). Counter-insurgency redux. *Survival*, *48*(4), 111-130.

[105] Brown, R. (2009). Public Relations and the Social Web: How to use social media and web 2.0 in communications. Kogan Page Publishers.

do this, the security of individuals, organisations and the general public would be negatively affected.

3.2 Use of Social Media to Counter Propaganda

Propaganda refers to deliberate acts undertaken to influence the attitudes of an individual or a group of people by use of various communication tools in expectation of getting particular reactions from the people that are in line their motives[106]. With the advent of social media networking platforms that are capable of reaching a vast audience within a blink, various individuals and groups both legal and illegal are exploiting these networks to actualize their motives with ease[107]. However, despite these platforms being utilized for ill motives of spreading unwarranted information, they have also presented suitable avenues that if well utilized can curb and reduce spread of false information and propaganda[108].

A good example of how social media is used to counter propaganda is in the fight against terrorism. In the contemporary era where terrorism is a major global threat, states are utilizing social media networks to spread anti-terrorist messages and to erode and neutralize the image of a mighty fortress of the terrorist organisations and criminal gangs[109]. For instance, in counter-terrorism campaigns, to erode the image of groups being mighty, security agencies can conduct loud and clear advertising of the incarcerations of the terrorist members, they can publicize their confessions, and of any act that indicate their lack of loyalty to the groups and to their colleagues, and any other measures that cast a mistrust over the terrorist's heroic image of fallen or captured members[110].

Apart from anti-terrorism campaigns, social media networks are also extensively used counter spread of false news[111]. Social networks are key channels that can be utilized to guard the

[106] Kalçık, A. P. D. T., & Bayraktar, Ü. A. (2017). Terror Propaganda on Social Media: Daesh Terrorist Organisation. International Journal of Business and Social Science, 8(9), 128-137.
[107] Kalçık, A. P. D. T., & Bayraktar, Ü. A. (2017). Terror Propaganda on Social Media: Daesh Terrorist Organisation. International Journal of Business and Social Science, 8(9), 128-137.
[108] Brown, R. (2009). Public Relations and the Social Web: How to use social media and web 2.0 in communications. Kogan Page Publishers.
[109] Ronfeldt, D., & Arquilla, J. (2001). Networks, netwars and the fight for the future. First Monday, 6(10).
[110] Manjoo, F. (2004). A Picture is no Longer worth a Thousand Words.
[111] Silverstein, B. (1987). Toward a science of propaganda. *Political Psychology*, 49-59.

reputation of a nation and to curb propagation of unwarranted information[112]. This is achieved through provision of true and accurate data on the prevailing situation to neutralize the unjustified information being spread[113]. In a similar manner to counter propaganda, social media platforms are also widely used by organisations to protect their images by countering spread of false information meant to tarnish the image of the organisations. This helps to bring credibility to the organisation and to preserve its image to the general public[114]. In this regard a large number of large organisations have put in place social media teams that are charged with the responsibilities of monitoring how the organisations are perceived by the public to monitor what the public thinks and say about the organisations. This put the organisations in a suitable position to respond immediately and provide factual data when faced with attacks that are likely to interfere with their reputation.

3.3 Use of social media for news management

In the contemporary era, governments across the world have realized the significance of social media and have incorporated them in their day to day operations. Various social networking sites such as Facebook, Twitter, and YouTube are widely used by state agencies to improve service delivery and to foster communication with the citizens. Social media platforms have emerged as the preferred means of reaching and engaging with the masses, culminating in exponential amplification. These networks are widely used by the governments for strategic communication, to clarify government policies and principles and to set the records straight on contentious matters. Traditionally, the governments utilized social media platforms as a key means of providing static information through direct hyperlinks or to offer applicable updates on agencies. As social networking has evolved, the government is viewing social media platforms more as tools rather than mandated "e-government" initiatives for delivery of services to the public.

One of the key uses of social media by the state security agencies is to manage and counter messages spread by terrorist organisations. Terrorist organisations have always adopted new and

[112] ibid
[113] PrenticeS.,HuffmanE., 2008. Social Media's New Role in Emergency Management, Idaho National Laboratory, INL/CON--07--13552
[114] PrenticeS.,HuffmanE., 2008. Social Media's New Role in Emergency Management, Idaho National Laboratory, INL/CON--07--13552

sophisticated technologies to promote their purposes and to popularize their ideologies[115]. These organisations have also managed to use social media for recruitment purposes across the globe and for championing their activities for various. For instance, due to the wide coverage of social media platforms, terrorist organisations have been able to communicate radicalizing messages to a far wider circle of potential adherents as compared to what would be the reach with the traditional media tools. Previously, the terrorist groups conducted radicalization through personal contact[116]. Also, some decades ago, when global jihadist movement was in its infancy, the followers of radical clerics circulated their sermons on audiotapes, reproduced one at a time and passed from one follower to another[117]. However, in the new era of social media, the jihadists can easily communicate and interlink from all corners of the world. This pose a great challenge to governments across the world as terrorism has emerged as one of the main threats to national security and economic and social progress.

Initially, governments were caught off-guard by the sophisticated technologies used by terrorist organisations and other criminal gangs[118]. However, they have realized that carrying out online campaigns through the social media networks is an effective measure that can be used to counter the threats posed by the terrorist organisations. One element of governments' response has been counter-messaging. This is an attempt by the government to refute or undercut the messages propagated by criminal gangs, terrorist groups and their sympathizers. In addition, through social media analysis, the state security agencies have the potential advantage of identifying individuals, networks, virtual communities, tactics, and specific types of content and language that promote and encourage violence[119]. Such analysis helps to identify certain indications of economic, political, social or cultural factors that are seen as the key sources of insecurity that spread in a social environment in which extremism can grow, and which may include collective narratives of grievance, social alienation, de-legitimizations of the state and radicalizing dogmas

[115] Thompson, R. L. (2011). Radicalization and the use of social media. *Journal of strategic security*, *4*(4),9.

[116] Ferguson, N., & Binks, E. (2015). Understanding radicalization and engagement in terrorism through religious conversion motifs. *Journal of Strategic Security*, *8*(1), 2.

[117] Dupuy, T. (2016). Once upon a time: re-thinking the fight against extremists. *Skeptic (Altadena, CA)*, *21*(2), 51-54.

[118] Kohlmann, E. F. (2006). The real online terrorist threat. *Foreign Affairs*, 115-124.

[119] Waldman, S., & Verga, S. (2016). *Countering violent extremism on social media*. Retrieved August 25, 2018, from Defence Research and Development Canada : http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

that revere, glamorize, or offer of rewards for violence[120]. In addition to this, it also makes it easier to ascertain and understand online social networks that support the organized coordination of criminal activities[121].

Social media networks also enable security agencies to measure and describe the nature of social ties networks in the hopes of better understanding and even envisaging their connection to individual actions. This can be done on online activities datasets activities which include participation in blogs and online discussion boards. Social media analysis can also assist in showing the number of people in an online social media networking site, the type of information shared among them and structures through which influence is exerted[122]. Social media analysis can therefore be helpful in explaining how motivations, ideologies and information flow among terrorists and criminal gangs and to give warnings of when these groups are expanding their scope and operations[123]. In addition to the above, the government security agencies can monitor patterns and themes of communications shared via social media platforms which help to provide them with crucial information regarding the mood and perceptions of citizenry an endeavor that is impossible with the utilization of past communications like surveys through phones or emails.

3.4 Social Media Surveillance and monitoring

The capability to predict future strategic and tactical contexts is of great importance in a bid to reduce the possibilities of being caught unawares by threats and to increase the resilience to them. In this respect, monitoring and surveillance have emerged as key components of the public sector. In the past, monitoring and surveillance involved signalizing relevant developments in the physical environment, for instance example in the domains of safety, education, and environmental policies. Currently, increased use of the internet and more precisely the social media networking platforms by the citizens, the associated security threats, and the likelihood of

[120] Waldman, S., & Verga, S. (2016). *Countering violent extremism on social media*. Retrieved August 25, 2018, from Defence Research and Development Canada : http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

[121] Waldman, S., & Verga, S. (2016). *Countering violent extremism on social media*. Retrieved August 25, 2018, from Defence Research and Development Canada : http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

[122] Prentice S., Huffman E., 2008. Social Media's New Role in Emergency Management, Idaho National Laboratory, INL/CON-07-13552

[123] Waldman, S., & Verga, S. (2016). *Countering violent extremism on social media*. Retrieved August 25, 2018, from Defence Research and Development Canada : http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

strategic surprises have prompted state security agencies to design a number of online surveillance strategies.

Social media platforms have enabled the security agents to track transactions and movements of individuals online, to intercept communications, and to read and interpret data. These platforms have emerged as invaluable resources for the benefit of the security agencies since the users of these sites leave marks about their identity, abilities, predilections, movements, contacts among others which can easily be gathered and analysed. A progressive and critical surveillance of social media sites can be conducted as a warning tool in case of present potential threats to national security, since the use of social networking sites by criminals, adversary states and other competitors is more and more increasing[124]. For this reason, progressive analysis of social media platforms by security agencies can serve as an early warning which can help to promote national security.

On top of the above, advancement in technology has equally enabled development on various tools that help monitor online communication[125]. Governments have increased surveillance in various social media platforms, ostensibly to discover new information that is detrimental to the security of the country. Governments argue that it's important to collect relevant online information because it helps to improve people's security and public safety as well as protecting people and curbing crime, thus enhancing national security[126] . With the rise and widespread use of social media, a lot of companies have emerged across the world that offer social media monitoring software that can be used by the government security agencies to monitor and sift through the vast amount of information created and shared through social media platforms. By use of these software, the government officials are not only able to aggregate, filter, and analyze the vast information shared on social media platforms on a daily basis but are also able to trace the exact location from which the social media communications are made and to monitor the potential of the people creating the posts of compromising security. Through various social

[124] Lyon, D., & Trottier, D. (2013). Key features of social media surveillance. In *Internet and Surveillance* (pp. 109-125). Routledge.

[125] Sutton, J.N., Spiro E., Butts C., Fitzhugh S., Johnson B., Greczek M., 2013. Tweeting the Spill: Online Informal Communications, Social Media, and Conversational Microstructures during the Deepwater Horizon Oilspill. International Journal of Information Systems for Crisis Response and Management 5-1: 58– 76

[126] Allmer, T., Fuchs, C., Kreilinger, V., & Sevignani, S. (2014). Social net working sites in the surveillance society. *Media, Surveillance, and Identity: Social Perspectives*, 49-70.

media platforms such as Facebook, Twitter, Instagram, YouTube, Google+, Foursquare, Reddit, Vine, Tumblr, Periscope, and several others, the security agencies are able to carry out a cybernetic investigation of all occurrences[127].

Use of social media surveillance has achieved a lot in the fight against terrorism and online platforms such as Twitter, Facebook, Instagram among others have played key roles in the fight against terrorism and insurgency. These platforms are now key tools utilized by the security agencies across the world to ask for and receive instant information from the general public and also to offer a suitable monitoring platform. Through adoption if these platforms, the security agencies are able to enhance the resilience of crowded places and to combat such acts such as terrorist attacks and also helps in fostering better coordinated information flow among various agencies in charge of national security as well as ensuring faster and effective communication between the security agencies and the public.

During terrorist attacks, social media have been effectively utilized by the security agencies to give the public updates. Examples of this are the attacks in Nice, Munich, Brussels and Berlin in 2016 as well as in London, Stockholm, Manchester and Barcelona in 2017 where social media platforms were widely and effectively used to keep the people informed of the occurrences on a regular basis in various languages[128]. In these incidents, police used social media platforms especially twitter to communicate practically with the general public which enabled the people to follow developments with ease[129] . Through online communication, security forces are also able to advise the general public to keep off crowded places and spots that are likely to be attacked. A good instance occurred during the Munich attack whereby the security forces gave warnings on the whereabouts of the perpetrators and warned the public to avoid specific locations[130].

[127] Brown, I. (2015). Social media surveillance. *The international encyclopedia of digital communication and society*, 1-7.

[128] Rauchfleisch, A., Artho, X., Metag, J., Post, S., & Schäfer, M. S. (2017). How journalists verify user-generated content during terrorist crises. Analyzing Twitter communication during the Brussels attacks. *Social Media+ Society*, *3*(3), 2056305117717888.

[129] Spaziante, L. (2017). The logic of sensorial effectiveness. Amateur videos, media witnessing, global crisis news. *Versus*, *46*(1), 17-40.

[130] Galily, Y., Yarchi, M., & Tamir, I. (2015). From Munich to Boston, and from theater to social media: The evolutionary landscape of world sporting terror. *Studies in Conflict & Terrorism*, *38*(12), 998-1007.

Social media significance in surveillance been acknowledged by Krebs who argued that if only effective monitoring and social media had been done, the 9/11 could have been prevented. Much was learnt from that occurrence and currently, security agents and intelligent teams routinely gather data and information to detect relationships and to try to ascertain potential individuals and groups that are threats took security[131]. After the 9/11 terrorist attack, social media surveillance and analysis has been widely used in the anti-terrorism campaigns[132] in detection and investigation of fraud and in disaster and fraud management[133].

3.5 Use of social media for Psychological Operations and public Diplomacy

Psychological operations, also known as PsyOps[134]can be underscored through the utilization of social media networks. Obviously, these operations are to disseminate messages that seek to have an impact on peoples' objective reasoning, motives and emotions[135]. Different agencies within the security spectrum conduct psychological operations on social media owing to the fact that there exists a large audience there. The primary aim is to influence the opinions of the large mass in a given direction that supports national security if a country. In the modern era, security agencies are taking advantage of the vast audiences on social media platforms to conduct psychological operations in a context of information warfare with the key aim of influencing the sentiments of the people such as emotions, motives, and objective reasoning.

The concept of psychological operations is not new. It has been utilized in various occasions in the past by the security agencies particularly the military to diffuse information to interfere with opponents divulging propaganda and artifact messages. This involves conveying messages to specific target groups to foster particular themes that result in desired attitudes and behavior that affect the attainment of political and military aims[136]. In the modern era, psychological operations have been well contextualized in security campaigns due to the cutting-edge

[131] Krebs V.E., 2002. Mapping Media of Terrorist Cells. Connections 24(3), 43-52

[132] ibid

[133] Hecker M., Vanbremeersch N., De Durand M., Souchet T., 2012. Nature et conséquence des réseaux sociaux pour les forces armées. http:// www.defense.gouv.fr/ content/download/204906/ 2271215/file/EPS2012- Reseaux sociaux.pdf

[134] Kilcullen, D. (2006). Counter-insurgency redux. *Survival*, *48*(4), 111-130

[135] ibid

[136] 9US Joint Publication 3-13.2. Psychological Operations, 07 January 2010, page V-2 can be found on: http://www.fas.org/irp/doddir/dod/jp3-13-2.pdf

technological innovations at the disposal characterized by the Internet, virtual reality, blogs, video games, and chat bots among others[137].

Social media platforms are also widely used by governments across the world to allow free access to information by the public, to spread democratic values and ideas, and to curb spread of misinformation by the criminals which have the potential of impacting on national security. The key ways through which this is achieved is use of blogs, Facebook posts, emails and Twitter which allows the public to source information and to give their views on political, economic and social discourses. Through constant communication with the public via social media platforms, the state organisations are not only able to influence the people but also to create a good rapport with the people which is a big boost to promotion of national security. In most cases, when security agencies directly collect information from the general public, it allows quick reaction while at the same time enhances the quality of their relationship with the people[138]. This enables the people to feel they are given participatory roles in the protection of the communities and the nation where they belong.

3.6 Social media and emergency and crisis management

Social media enable increased communication and connections among millions of users globally and have emerged inevitable components of the day to day lives for many people[139]. These platforms attract a large number of users and have thus become suitable and effective mediums of dissemination of information. As a result, state security organisations and disaster prevention and management teams have found them as effective tools to use in managing crisis events.[140] As it is evident, in the modern era, governments and security agencies widely utilize social media platforms for management of emergencies and disasters.

[137] Kilcullen, D. J. (2006, September). Three pillars of counterinsurgency. In *US Government Counterinsurgency Conference* (Vol. 28).

[138] Wybo, J. L., Fogelman-Soulié, F., Gouttas, C., Freyssinet, É., & Lions, P. (2015). Impact of social media in security and crisis management: a review. *International Journal of Emergency Management*, *11*(2), 105-128.

[139] Reuter, C., Hughes, A. L., & Kaufhold, M. A. (2018). Social media in crisis management: An evaluation and analysis of crisis informatics research. *International Journal of Human–Computer Interaction*, *34*(4), 280-294.

[140] Harrald, J. R., Egan, D. M., & Jefferson, T. (2002). Web enabled disaster and crisis response: What have we learned from the September 11 th. In Proceedings of the Bled eConference (pp. 69–83). Retrieved from https:// domino.fov.uni-mb.si/ proceedings.nsf/ proceedings/ d3a6817c6cc6c4b5c1256e9f003bb2bd/ $file/harrald.pdf

Since 2006, the use of social medial networks in crisis and disaster management has gained increasing interest and is widely used to disseminate information and to receive feedback from the public[141]. A good social media platform that is widely used during emergencies is Facebook. It has become a vital communication channel during emergencies and crises whereby people are notified of the events through posts and they are offered a platform to share support and resources. Facebook is also widely used to train the public on security and conflict prevention. This is mostly done by community managers who manage the accounts belonging to public authorities and private companies with a well outlined strategy.

In most crisis management instances, social media platforms are used to broadcast vital information, to rectify misinformation and to build situational awareness. For instance, these platforms were widely used to converse and engage with communities around the globe during the Hurricane Harvey and Imma. Facebook, Twitter and instagram posts helped in informing the people across the world about the hurricanes and its aftermaths. At the same time, apart from informing the people about the disasters, the social media networking platforms also encouraged people to support relief efforts. Volunteers from all corners of the world used the platforms to provide help to the affected areas by use of pertinent real time information of who actually needed help.In another instance, social media networks were used by the Los Angeles Fire Department to provide information to the public and to get information from the people. In addition to the above, security agencies also utilize social media networks during occurrences that threaten public order and security. An example of this occurred during the 2011 riots in Great Britain whereby Twitter was effectively used to control and contain the situation.

3.7 Social Media Use in Investigation and Cyber Crime Prevention.

Technology has enabled people to shift towards online platforms that allow them to share private information with individuals unknown to them globally. Criminals have also found social media platforms as suitable avenues of panning and coordinating their activities. It is evident that in the modern era, the methods criminals leverage in an attempt to plan, organize and commit crimes

[141] Hagar, C. (2013). Crisis informatics: Perspectives of trust – is social media a mixed blessing? *SLIS Student Research Journal*, *2*(2). Retrieved from http://scholarworks.sjsu.edu/slissrj/vol2/iss2/2

are changing rapidly and there is a shift from traditional tactics to the establishment and use of social media platforms[142].

Currently, criminal gangs are utilizing more sophisticated approaches and technologies to coordinate their operations key among them being Twitter, Facebook, Instagram and YouTube. They to a large extent utilize these platforms to organize, advertise, and publicize their illegal trades. Currently, planning and coordination of all sorts of crimes ranging from drug trafficking to prostitution among other crimes is happening via social media sites which implies that if detectives and security intelligence units are not online tracking these illicit activities, then there is a big gap in the fight against insecurity[143]. This revolution in crime perpetration is a clear indication that digital interaction is posing challenges to law enforcement agencies to keep pace with many of them turning to social media platforms to help in investigations[144].

While criminals have found social media as suitable platforms to promote their dealings, they have however forgotten that their digital footprints last forever on the online platforms which make these platforms suitable platforms for security agencies to track criminals. It is evident that social media platforms are effective tools for investigations and law enforcement. Similar to other internet services, social media platforms are widely utilized as extra sources of information in various types of investigations where they are used to identify the potential perpetrators of crime and to gather information about the suspects and the victims[145]. In the modern era, spending hours trying to physically follow up on leads is becoming outdated and the security agencies that are still relying on these tactics are missing huge investigative opportunities and leads by not incorporation social media platforms in their undertakings[146].

Cybercrime that touch on infringement of physical persons as well as individual properties continue to be combatted through the use of social media sites. Social media platforms constitute

[142] Lynch, M. (2002). The culture of control: Crime and social order in contemporary society. *PoLAR: Political and Legal Anthropology Review*, *25*(2), 109-112.
[143] Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).
[144] Lynch, M. (2002). The culture of control: Crime and social order in contemporary society. *PoLAR: Political and Legal Anthropology Review*, *25*(2), 109-112.
[145] Trottier, D. (2012). Policing social media. *Canadian Review of Sociology/Revue canadienne de sociologie*, *49*(4), 411-425.
[146] Innes, M. (2012). 'Signal crimes': detective work, mass media and constructing collective memory. In *Criminal Visions* (pp. 63-82). Willan.

an important real time source of intelligence and information that can be used to fight cybercrime. According to Crump, social medial are suitable platforms on which security agencies can set up communication and reaction strategies in the fight against cybercrime. This indicates that social media platforms apart from serving the basic function of communication and interaction, they also play a key role in crime investigations and prevention[147].

[147] Trottier, D. (2012). Policing social media. *Canadian Review of Sociology/Revue canadienne de sociologie*, *49*(4), 411-425.

CHAPTER FOUR

DATA ANALYSIS AND PRESENTATION

4.1 Introduction

This chapter presents data analysis, presentation of the findings, and discussion of the findings. The main objective if the study was to analyse the impact of social media on national security in Kenya. This chapter is structured according to the objectives of the study. The analysis is done using descriptive statistics such as means, standard deviations, frequencies and percentages and inferential methods. The findings are presented in form of tables and charts, and graphs.

4.2 Response Rate

The study targeted to collect data from 83 employees at Communication Authority of Kenya, The study administered 83 questionnaires out of which 54 were dully filled and returned making a response rate of 65.1%. According to Kothari[148] a response rate higher than 50% is considered sufficient to yield reliable results. In this case, the response rate was higher than 50% and therefore the findings are considered sufficient to yield reliable conclusions. The response rate is presented in the chart below

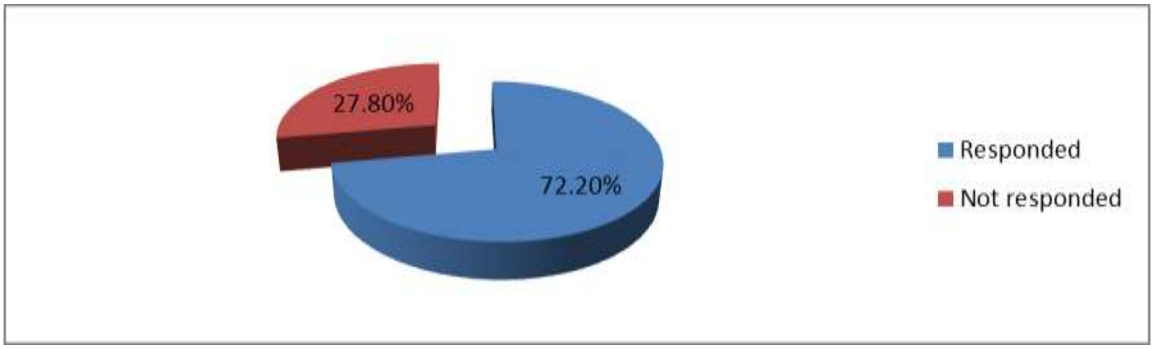

Figure 4.1: Response Rate

[148] Kothari, C. R. (2001). *Research Methodology Methods and Techniques* (2nd ed.). New Delhi, New Age International.

4.3 Demographic Information

In this section, the study sought to determine the demographic information of the respondents. Here, main focus was on the gender of the participants, age, the highest level of education attained, the departments in which they served, and the duration they have worked at the organisation.

4.3.1 Gender

The researcher first endeavored to establish the gender of the respondents who took part in the study. The findings are shown below;

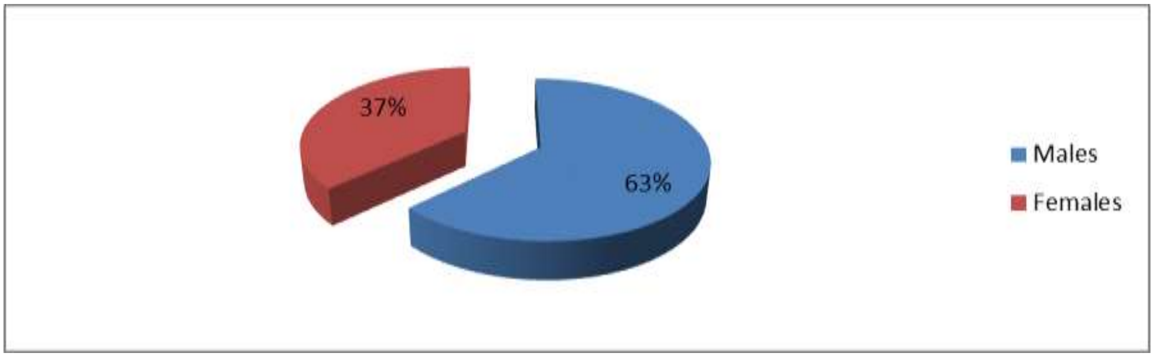

Figure 4.2: Distribution of the respondents by gender

The results shown above indicate that 63% of the respondents were males while 37% were females. It is clear from the findings that majority of the participants were males.

4.3.2 Age

The aim of analysis here was to determine the distribution of the respondents by age. The results are summarised below;

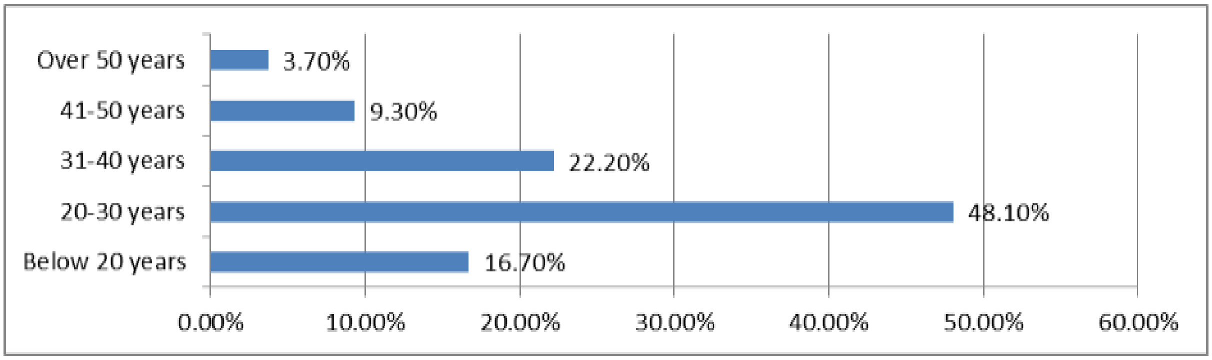

Figure 4.3 :Distribution of the respondents by age

The findings in figure 4.3 above show that 48.10% of the respondents were aged between 20-30 years, 22.20% were aged between 31-40 years, 16.70% were below 20 years, and 9.30% were aged 41-50 years, while 3.70% had over 50 years. Based on the findings, it is clear that the majority of the respondents were young.

4.3.3 Education Level

In this section, the study sought to determine the highest education level attained by the respondents. The findings are presented as below;

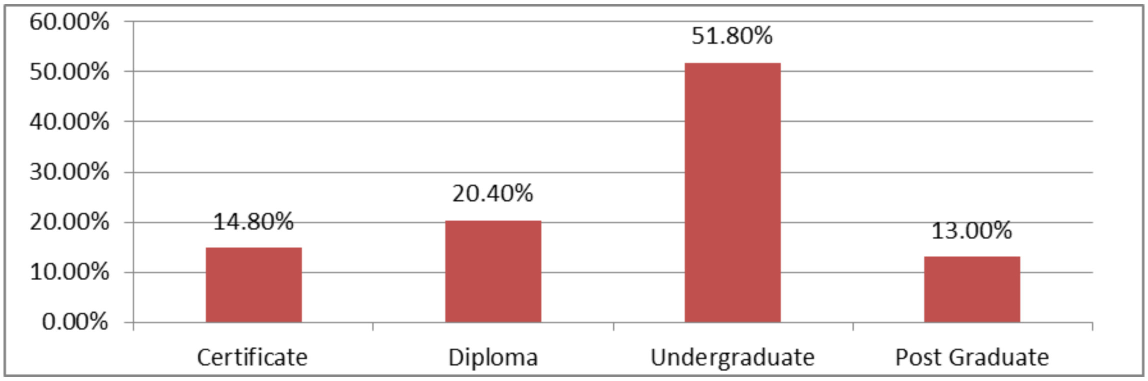

Figure 4.4: Highest education attained by respondents

Based on the analysis findings in figure 4.4 above, the majority of the participants (51.80%) were undergraduates, 20.40% had attained diplomas, and 14.80% had attained certificates, while 13.0% of the respondents had post graduate degrees. From the findings, it can be deduced that the respondents were well educated and were in a good position to offer the required data and information.

4.3.4 Department

Here, the aim of the analysis was to determine the various departments in which the respondents served. The findings are presented as below;

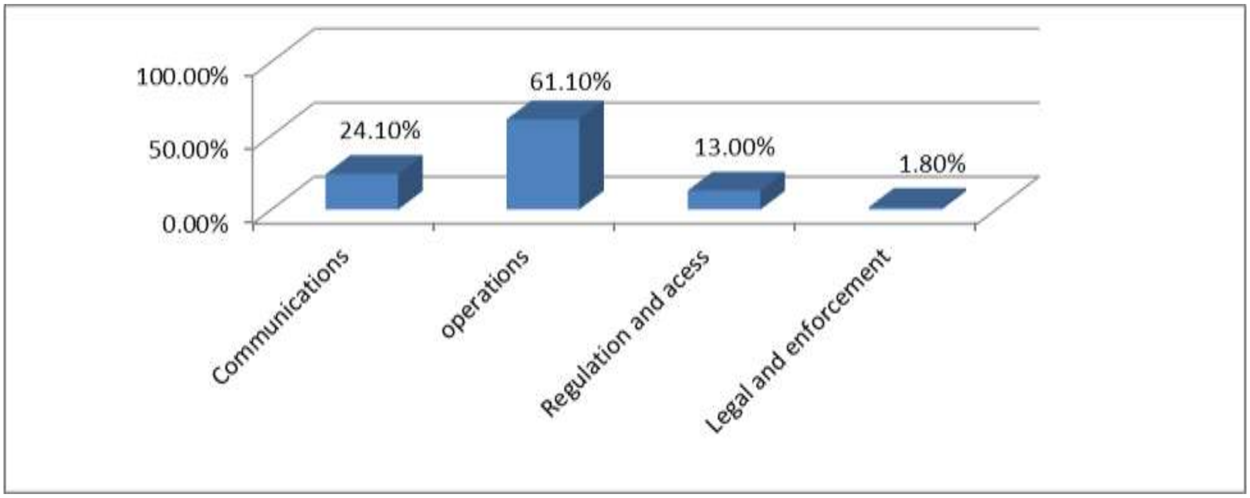

Figure 4.5: Department

4.3.5 Duration Worked at the Organisation

In this section, the study sought to determine the duration the respondents had worked in the organisation. The findings are presented as below;

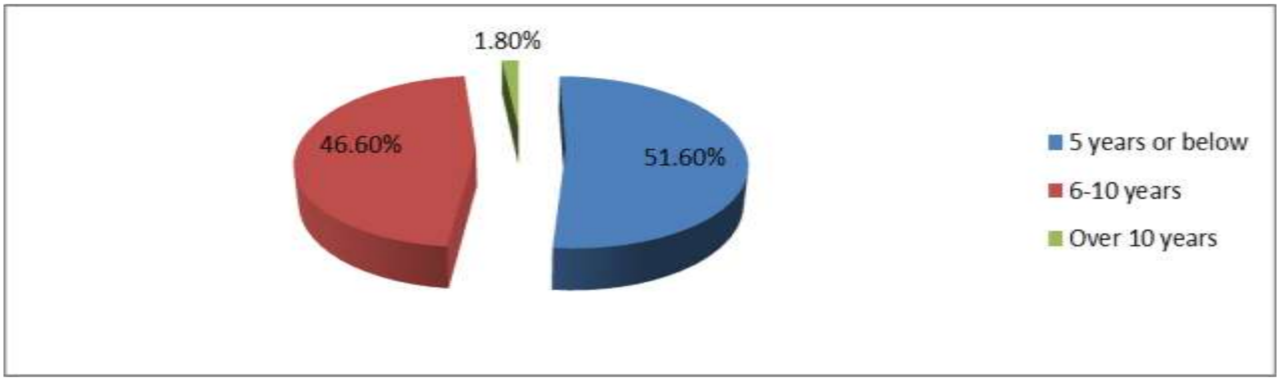

Figure 4.6: Duration the respondents had worked at CAK

The findings in figure 4.6 above indicate that 55.60% of the respondents had worked in the organisation for 5 years and below, 46.60% had worked at the organisation for 6-10years, while a small proportion of the respondents had worked at the organisation for over 10 years. While those who had worked for 5 years and below had the highest proportion, there was no statistically significant difference between this group and those who had worked at the organisation for 6-10 to 10 years. The findings therefore indicated that the respondents had served the organisation for a considerable duration of time and were thus well positioned to offer reliable data for the study.

4.4 Threats of Social Media to National Security.

The study sought to analyse social media as a threat to national security. Specifically, the study determined the state of the national security with regard to social media, the extent to which social media has led to insecurity in the country, the various ways terrorist and criminal groups utilize social media, and frequency of cyber-crimes in Kenya.

4.4.1 Social Media as a Threat to National security

To start with, the study requested the respondents to give their opinion on whether they consider social media a threat to national security or not. The findings are presented in the figure below;

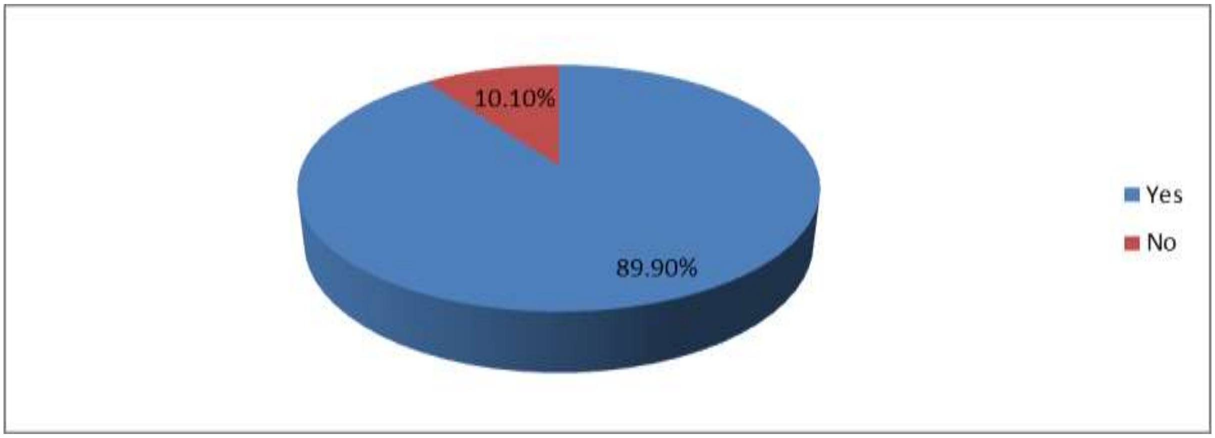

Figure 4.7: Social media as a threat to national security

From the analysis findings presented in figure 4.7, the majority of the respondents (89.90%) agreed that social media is a threat to the security of the nation while a small proportion of 10.10% denied that social media does not pose any threat to the national security. Similar findings were obtained from the members of the public who reported that social media is a threat to the security of the country since currently most crimes are planned and coordinated through online interactions. The findings were in agreement to the results of a study undertaken by Kimutai[149] whereby the majority of the participants (93%) were in agreement that social media is a threat to national security while only a small proportion of 7% denied.

4.4.2 The State of the National Security with Regard to Threats from Social Media

The study sought to determine the state of Kenya's national security with regard to threats from social media. The findings are presented in the figure below;

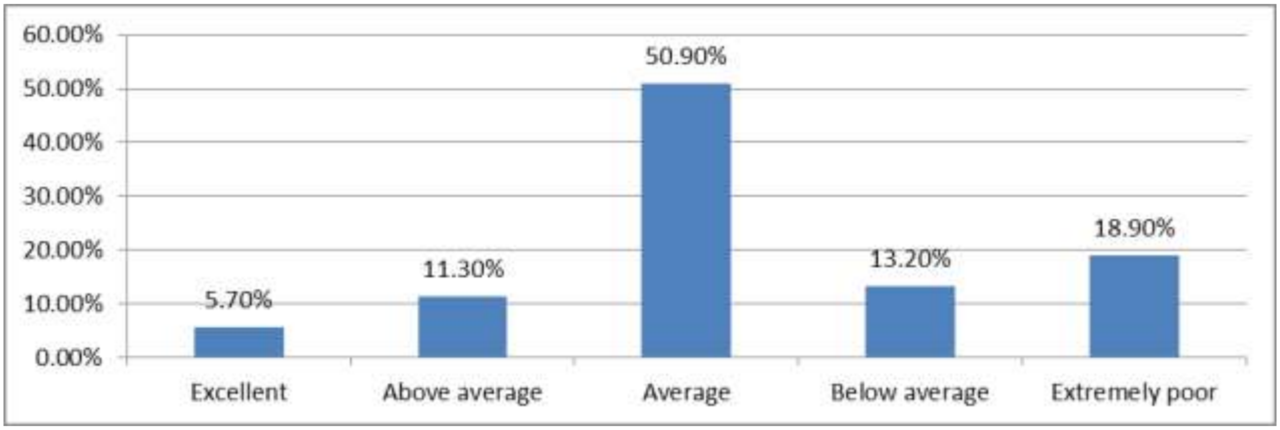

Figure 4.8: State of Kenya's national security with regard to social media

From the findings in the figure 4.8 above show that the majority of the respondents (50.90%) felt that the security situation in Kenya in relation to social media is average, 18.90% felt that the security of the nation is extremely poor, 13.20% felt that the security of the nation is below average, 11.30% reported that the security is above average while a small proportion of the respondents reported that the security situation in Kenya in relation to social media is excellent.

[149] Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya.* Retrieved April 3, 2018, from UONBI: erepository. uonbi.ac.ke/.../ Kimutai_Social%20Media%20And% 20National%20Securit...

This was in line with the views of the members of the public who reported that the situation of the country is average with regard to social media. The findings are in agreement to the result of a study conducted by Kimutai whereby the majority of the military officials sampled reported that the security of Kenya in relation to social media is average.

4.4.3 Extent to Which Social Media has led to Insecurity in Kenya

The study sought to rate the extent to which social media has contributed to various forms of insecurity in Kenya. The analysis findings are presented in the table below;

Table 4.1: The extent to which social media has contributed to various forms of insecurity in Kenya

Forms of Insecurity	Mean	Std. Deviation
Terrorism	3.1852	1.50564
Hate speech	4.8333	1.42308
Information warfare	3.2963	1.36851
Tribal clashes	3.7778	1.43299
Cattle rustling	2.3704	1.43140
Poaching	3.0556	10.04095

From the findings in table 4.1 above, the respondents reported that social media platforms are used to a great extent to facilitate hate speech (M=4.8333). In addition to this, they reported that social media platforms are used on a moderate extent to facilitate terrorism (M=3.1852), Information warfare (M=3.2963), Tribal clashes (M= 3.7778), and poaching (M=Poaching). Further, the respondents reported that social media networks are used to a low extent to facilitate cattle rustling (M=2.3704). The findings from CAK were in line with the information obtained from the DCI and NSI. According to the DCI respondent, criminal and terrorist organisations misuse social media platforms to propagate unwarranted information, to plan and coordinate crime, hate speech among other ill motives.

4.4.4 Various Ways Criminal Groups utilize Social Media

The study sought to determine the extent to which criminal groups utilize social media to facilitate various crimes. The findings are presented in the table below;

Table 4.2 : Uses of Social Media by criminal Groups

Uses of Social Media by Criminal Groups	Mean	Std.
Criminal organisations use social media to spread viruses	3.0926	1.59325
Criminal organisations use social media to smuggle drugs	3.2222	1.58302
Criminal organisations use social media to facilitate human trafficking	2.8519	1.75549
Criminal organisations use social media to facilitate money laundering	3.5556	1.60972
Criminal organisations use social media to spread and promote pornography.	3.9630	1.50425

From the findings in table 4.2 the respondents reported that criminal groups to a low extent utilize social media platforms to spread viruses (M=3.0926), smuggle drugs (M=3.2222), to facilitate money laundering (M=3.5556), and to spread and promote pornography (M=3.9630). In addition, the respondents reported that criminal groups use social media to a low extent to facilitate human trafficking. Similar views were obtained from the DCI. According to the DCI official, criminal gangs particularly in urban centres utilize social media sites to communicate and plan their operations.

"Gangs in urban centres such as the *gaza* which mostly operate in Eastlands use social media to flaunt their criminal activities. They do this to make them look heroic" (DCI respondent, 2018)

"Social media platforms are used to a large extent by cartels to smuggle drugs and goods and to recruit distributers" (NIS, 2018)

4.4.5 Social Media as a Tool Used by Terrorist Organisations

The study sought to determine whether terrorist organisations utilize social media as tools to threaten national security. The findings are presented in the chart below;

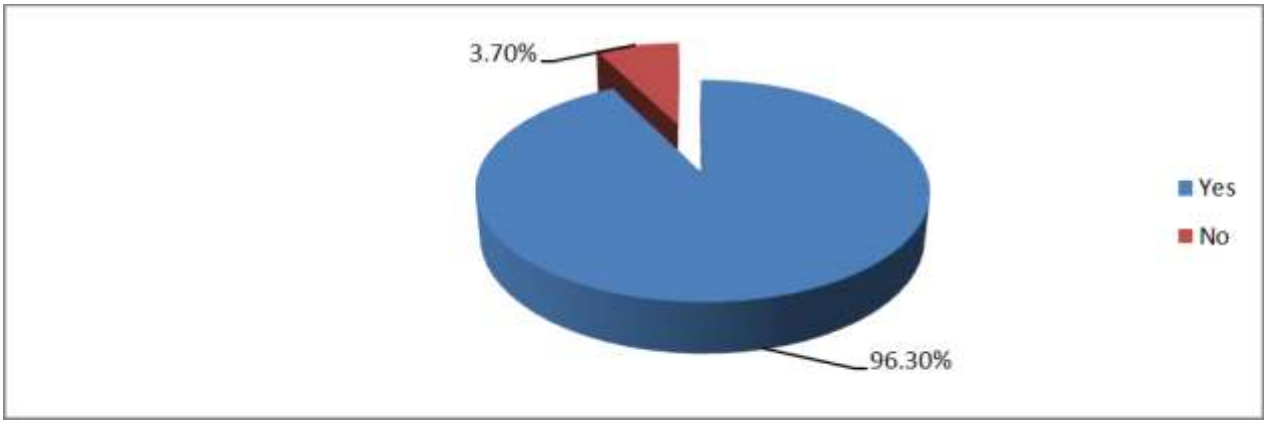

Figure 4.9: Social media use by terrorists

According to the results indicated above, almost all the respondents (96.30%) agreed that terrorist organisations utilize social media platforms to threaten the security of the nation. Only a small proportion of the participants (3.7%) denied that social media platforms are not utilized by terrorist organisations to facilitate their operations.

From the respondents who agreed that terrorist organisations utilize social media to facilitate their operations, the study further sought to determine the level of their agreement on the various uses of social media media by the terrorist groups. The findings are tabulated as below;

Table 2.3: Uses of social media by terrorist organisations

	Mean	Std. Deviation
Communication	2.1860	1.21999
Ideological Radicalization	2.1390	1.27720
Recruitment	2.8605	1.52099
Training	2.4419	1.50083
Violence	2.0930	1.44443

From the findings, the respondents agreed that terrorist organisations utilize social media mainly for recruitment purposes (M=2.8605), to facilitate training (M=2.4419), for communication purposes (M=2.1860), for ideological radicalization (2.1390), and to facilitate threats of violence (2.0930). Related findings were obtained from the DCI and NIS respondents who reported that terrorist organisations to a large extent to facilitate their operations. According to the DCI, Alshabab for instance highly utilize social media to spread propaganda, to coordinate attacks and to showcase their successful attacks in an effort to spread fear.

"Social media platforms are not only used by terrorist to publicize their operations. Some groups such as the Al Shabab rely on these networks to recruit new member and to raise funds from sympathizers" (NIS interviewee, 2018)

The findings are in line with the results of Kimutai[150] who established that terrorists utilize social media for communication purpose, threats of violence, ideological radicalization, spread of propaganda, coordination of operations and fund raising among other uses.

4.4. 6 Frequency of Cybercrime Incidences

The study sought to determine the frequency of cybercrime incidences in Kenya. The findings are presented in the figure below;

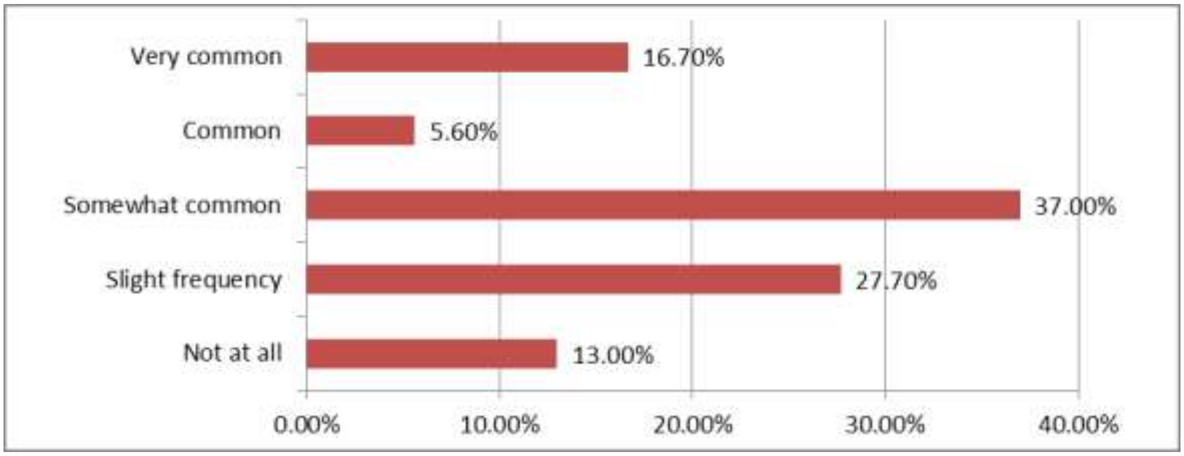

Figure 4.10: Frequency of cybercrime incidences in Kenya

From the findings above, 37.00% of the respondents reported that cybercrime incidences are somewhat common in Kenya, 27.70% reported that cybercrime incidences are slightly frequent in the country, 16.70% reported that cybercrime incidences in the country are very common, 13% of the respondents reported that cybercrime incidences do not occur at all while a small proportion (5.60%) reported that cybercrime incidences in Kenya are common.

[150] Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya.* Retrieved April 3, 2018, from UONBI: erepository. uonbi.ac.ke/.../ Kimutai_Social%20Media%20And% 20National%20Securit...

4.5 Use of Social Media to Prevent, Limit or Remove Threats to National Security

The purpose of this analysis was to find out the various ways in which social media platforms are used to limit or remove threats to national security.

4.5.1 Use of Social Media by the Government to Enhance National Security

The analysis in this section sought to determine whether the government uses social media to enhance national security. The findings are presented in the chart below;

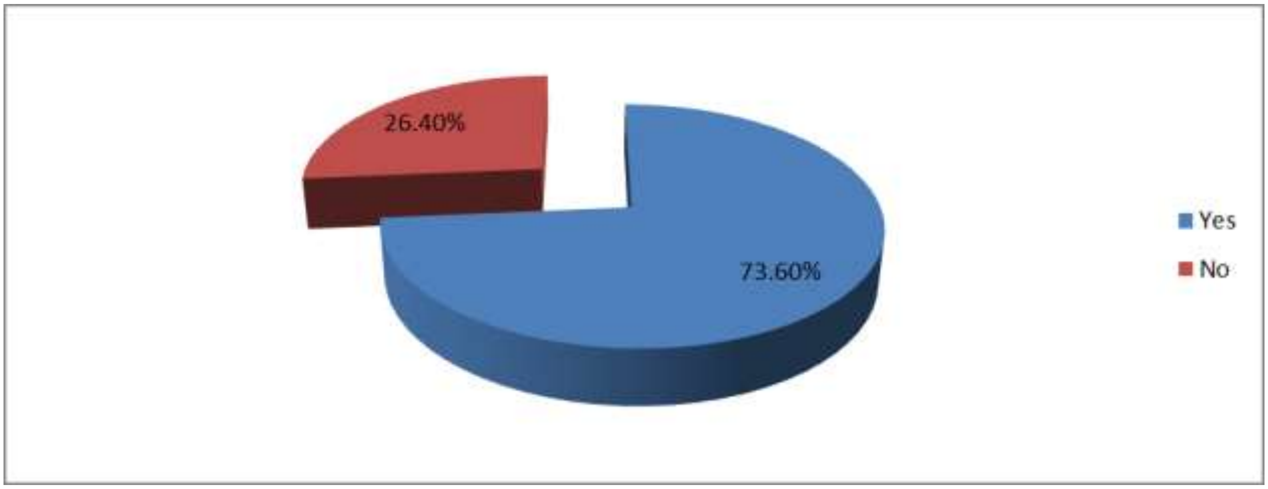

Figure 4.11: Use of social media to enhance national security

From the findings in figure 4.11, 73.60% agreed that the state security agencies use social media platforms to enhance national security. Only a small proportion (26.40%) denied. The findings were in line with the information obtained from the indepth interviews whereby the respondents reported the governments security agencies mainly the Kenya Police Service and the Directorate of Criminal Investigation utilizes social media particularly Twitter to interact with the public in an effort to foster community policing and to promote security. The findings are in agreement with the findings of Kimutai[151] who conducted a study on the effect of social media on national security among the military officials whereby the majority agreed that the security agencies in the country utilize social media platforms for security purposes mainly for surveillance.

4.5.2 Online Monitoring of Social Media Content

In this section the purpose of the analysis was to determine whether there is online monitoring of social media content. The findings are presented in the chart below;

[151] Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya.* Retrieved April 3, 2018, from UONBI: erepository. uonbi.ac.ke/.../ Kimutai_Social%20Media%20And% 20National%20Securit...

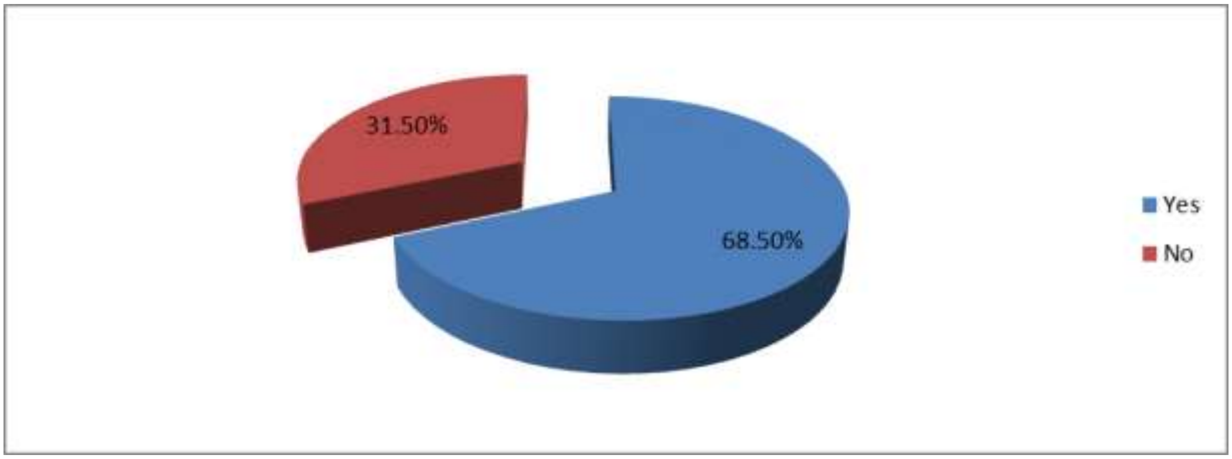

Figure 4. 12: Online monitoring of social media content

The findings in the chart above shows that the majority of the respondents (68.50%) agreed that there is online monitoring of social media content while 31.50% disagreed. In Kenya, the Communication authority of Kenya is charged with the role of monitoring the content shared online. However, the body does not do much in this regard. This concern was common among the general public whereby the respondents reported that the security bodies in the country only utilize social media for public relations purposes but they do not much to enhance national security as far as social media is concerned.

4.5.3 Use of Social Media by Security Agencies to Enhance National Security

The study sought to determine the various ways in which security agencies utilize social media. The findings are presented in the table below;

Table 4.4: Use of social media to enhance national security.

Statement	Mean	Std.
Security agencies mostly use social media to counter propaganda	3.1296	1.56671
Security agencies mostly use social media to promote public diplomacy	3.5000	1.39744
Security agencies mostly use social media for open source intelligence	4.1074	1.52363
Security agencies mostly use social media to communicate with the public.	4.1704	1.50842

From the findings, the respondents agreed that security agencies and government leaders use social media to communicate with the public (M=4.1704), security agencies use social media for open source intelligence (M=4.1074), security agencies mostly use social media to promote public diplomacy (M=3.500), and to counter propaganda (M=3.1296). A good instance of the use of social media to enhance national security is the use of social media by the Kenya police to interact with the public and to enhance community policing efforts in the country. Through a twitter handle @Policeke, the Kenya police have been better placed to interact with the people countrywide. This has to a large extent helped to improve the intelligence obtained by the Kenyan police while dealing with the security situation in the country[152]. Another government body that utilizes social media platforms to enhance national security is the Directorate of Criminal Immigration (DCI), through their twitter handle @ImmigrationDept; it keeps the public informed on key security issues and also gives the people a suitable platform to report crime. Other agencies that use social media platforms include the Ethics and Anti-Corruption Commission (EACC), which helps to inform and educate the people on matters of integrity and ethics. From the foregoing, it is clear that the government is in the right direction in the use of modern communication technologies such as social media platforms to enhance national security

4.6 Strategies Used to Curb and Minimize the Negative Effects of Social Media on the National Security

The third objective of the study was to determine the specific strategies devised to curb and minimize the threats of social media to national security. The key theme that dominated the responses is that the government has introduced cybercrime law. This act offers a framework for timely and effective detection, investigation and prosecution of cybercrimes such as unauthorized access to and interference of computer systems by third parties, propagation of pornographic content particularly involving children, cyber bullying, and publication of fake content and false information. These and other cybercrimes contained in the act attract very huge penalties and fines. For instance, publication of fake content attracts a fine of 5 million Kenyan shillings (USD$50,000) or a jail term of 10 years. Unauthorized intrusion and interference state protected computer systems attracts the longest jail term of 20 years. However, while this act can

[152] Atagana, M. (2013). Kenya’s Westgate attack: social media in the days of tragedy. Retrieved November 16, 2013, from http://memeburn.com/2013/09/kenyas-westgate-attack-socialmedia-in-the-days-of-tragedy/

contribute significantly in curbing misuse of social media platforms, it has various shortcomings. One of the key shortcomings is that the act is too vague when it comes to key issues especially those that deal with surveillance. Also, while the act is strict of prevention of hate speech, it is does not what exactly hate speech entails.

"There are no stringent measures in Kenya to curb crimes facilitated via social media. The social media bill has not been fully implemented and from the look of things, there is still a long way to go "(DCI official, 2018).

From this, it is clear that the government still has a lot to do in order to fully safeguard the national security from social media threats.

Another strategy reported by the respondents that national security agencies use to curb and minimize social media threats to national security is close monitoring of various groups formed on social media platforms and the content published and shared on social media platforms. The respondents reported that through the Communication Authority of Kenya, the government has installed and invested in quite sophisticated infrastructure and software to closely scrutinize social media platforms to ensure the country is safe. Through this, they authorities are able identify the malicious social media accounts and to suspend them. This is a key milestone in the fight against social media misuse. Another strategy used by national security agencies to minimize social media threats to national security is arrest and conviction of individuals involved. Currently, the security agencies are able to track down and arrest individual s who uses social media to interfere with the national security.

The respondents were further asked to give suggestions on how people can protect themselves against offensive use of social media and to improve the security situation of in the country. The respondents suggested that people should avoid bad conversations on social media platforms that are likely to trigger divide and intensify hatred, should avoid joining social media groups that do not have clear agenda and those with suspicious motives, to avoid spreading fake content and lies on social media sites, and to liaise with security agencies through reporting cases of social media misuse. In addition, the respondents reported that people other than just socializing and making connections, people should use social media platforms as effective tools for spreading peace. It should be people’s responsibility to utilize social media platforms to work towards promoting peace initiatives and supporting groups and individuals who are involved in peace process. The respondents further reported that social media users should post responsibly in order not to stir conflicts and bloggers should not just focus on making money and they should instead focus on posting content that does not cause insecurity. With regard to monitoring of social media content, the key respondents insisted that the security agencies and the relevant bodies should closely monitor the content shared through social media platforms.

CHAPTER FIVE

SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter presents a summary of the study according to the specific objectives. The chapter also presents conclusions and recommendations of the study.

5.2 Summary of the Study

The general objective of the study was to analyze the role of social media on national security with reference to Kenya. Specifically, the study sought to examine the impacts of social media usage to national security, to examine the use of social media by the security agencies in preventing, limiting or removing threats to Kenya's national security, and to evaluate the various strategies put in place to curb and minimize the negative effects of social media on Kenyan's national security.

With regard to the impact of social media on national security, the study established that social media is actually a threat to national security. It was established that criminals are taking advantage of the rapid advancement in the information and communication sector particularly the social media plan, execute and coordinate their activities. The respondents shows that social media platforms are used by local community criminal gangs to a great extent by criminals to facilitate hate speech, to facilitate information warfare, tribal clashes, to coordinate poaching activities, to facilitate cattle rustling. It was also established that terrorist utilize social media platforms to disturb the national security by using them as recruitment and training tools, to facilitate communication, for ideological radicalization and to facilitate threats of violence.

With regard to the use of social media by the security agencies to prevent, limit and remove threats of social media to national security, the study found out that the majority of the respondents agreed that the state security agencies use social media platforms to enhance national security. They mainly use social media to communicate with the public, for open source intelligence, to promote public diplomacy and to counter propaganda. The key government organisations that have notable presence on social media are the Kenya Police Service and the DCI. These bodies mainly use twitter handles to inform the public on security issues and they offer a suitable platform to the public where they can air their opinions and where they can report crimes. A large proportion of the respondents reported that there are bodies that are charged with the responsibility of social media content with Communication Authority of Kenya being in the frontline. However, concerns were raided that not much has been done when it comes to monitoring of social media content since most of these sites are still misused to facilitate criminal activities and there are numerous cases of cybercrime cases.

With regard to the strategies that have been put in place to curb and minimize the threats of social media to national security, the study found out that the cybercrime act is the most remarkable strategy as it provides a framework for timely and effective detection, investigation and prosecution of cybercrimes such as unauthorized access to and interference of computer systems by third parties, propagation of pornographic content particularly involving children, cyber bullying, and publication of fake content and false information. The study also found out that the government closely monitors various groups formed on social media platforms and the content published and shared on social media platforms to prevent publication of unwarranted content.

5.3 Conclusion

Based on the findings, a conclusion can be made that social media is a threat to national security. Terrorist organisations take advantage of social media platforms to facilitate ideological radicalization, recruitment and training, communication, to popularize their actions and to spread propaganda. Social media platforms are also used by community gangs to facilitate hate speech, money laundering, to facilitate information warfare, tribal clashes, to coordinate poaching activities, and to facilitate cattle rustling. The study also concludes that security agencies utilize to enhance national security. This is achieved through communication with the public, as a tool for open source intelligence, to promote public diplomacy and to counter propaganda. The key government organisations that mainly utilize social media for these purposes are the Kenya Police Service and the DCI. These bodies mainly use twitter handles to keep the people informed on security matters. The study further concluded that the government has put in place various strategies to minimize the threats of social media to the national security. These include the cybercrime act which offers a framework for timely and effective detection, investigation and prosecution of cybercrimes. The other strategy used to reduce threats of social media on national security is close monitoring of social media groups and content shared online.

5.4 Recommendations to the Study

Based on the findings of the study, the following recommendations are made;

i. Relevant government authorities should intensify social media surveillance and monitoring of content shared on these platforms in order to curb and minimize threats to national security.

ii. The government and various relevant bodies should focus on policy development and public awareness campaigns to sensitize the public on how to utilize social media platforms well to promote cohesion and peaceful coexistence.

iii. The government is recommended to put in place data protection and privacy policies. Data protection and privacy policies, which lack in most developing countries are essential for the maintenance of trust in the ICT platforms to ensure best practices in data protection and information security.

iv. The government should send law enforcement agents for special trainings to attain specialized technological skills on how to combat negative impacts of social media on national security.

References

Abdulhamid, S. M., Ahmad, S., Waziri, V. O., & Jibril, F. N. (2014). Privacy and national security issues in social networks: the challenges. *arXiv preprint arXiv:1402.3301*.

Abrahms, M., Beauchamp, N., & Mroszczyk, J. (2017). What terrorist leaders want: A content analysis of terrorist propaganda videos. *Studies in Conflict & Terrorism*, *40*(11), 899-916.

Aday, S., Henry F., Marc L., and John S. (2010), Blogs and Bullets: New Media in Contentious Politics. Peaceworks, no. 65 (2010). P.11.

Aggarwal, P., Arora, P., & Ghai, R. (2014). Review on cyber crime and security. *International Journal of Research in Engineering and Applied Sciences*, *2*(1), 48-51.

Alazab, M., Venkatraman, S., Watters, P., Alazab, M., & Alazab, A. (2012). Cybercrime: the case of obfuscated malware. In *Global Security, Safety and Sustainability & e-Democracy* (pp. 204-211). Springer, Berlin, Heidelberg.

Albrechtslund, A. (2008). Online social networking as participatory surveillance. *First Monday*, *13*(3).

Allmer, T., Fuchs, C., Kreilinger, V., & Sevignani, S. (2014). Social net working sites in the surveillance society. *Media, Surveillance, and Identity: Social Perspectives*, 49-70.

Atagana, M. (2013). Kenya's Westgate attack: social media in the days of tragedy. Retrieved November 16, 2013, from http://memeburn.com/2013/09/kenyas-westgate-attack-socialmedia-in-the-days-of-tragedy/

Awan, I. (2017). Cyber-extremism: Isis and the power of social media. *Society*, *54*(2), 138-149.

BBC. (2010). Israeli military 'unfriends' soldier after Facebook leak. Retrieved 9 March 2010, from http://news.bbc.co.uk/2/hi/middle_east/8549099.stm

Best, J.W. and Kahn J.V. (2006) Research in education. United States of America: Pearson.

Blitzblau S., (2011). Analisitecnicadellecapacità di NetINTdeigruppiterroristici, Information Warfare Conference 2010, Franco Angeli, Milano.

Bowman-Grieve L., (2010). A psychological perspective on virtual communities supporting terrorist & extremist ideologies as a tool for recruitment, Euro ISI Conference Submission, Leeds.

Brown, I. (2015). Social media surveillance. *The international encyclopedia of digital communication and society*, 1-7.

Brown, R. (2009). Public Relations and the Social Web: How to use social media and web 2.0 in communications. Kogan Page Publishers.

Brown, R. (2009). Public Relations and the Social Web: How to use social media and web 2.0 in communications. Kogan Page Publishers.

Carafano, J. J. (2009). All a twitter: How social networking shaped Iran's election protests. *Heritage Foundation Backgrounder, 2300*.

Coiera, E. (2013). Social networks, social media, and social diseases. *BMJ: British Medical Journal (Online), 346.*

Cragin, R. K. (2017). The November 2015 Paris Attacks: The Impact of Foreign Fighter Returnees. *Orbis*, *61*(2), 212-226.

Crunbase. (2018). *Communications Authority of Kenya.* Retrieved May 28, 2018, from Crunch base: https://www.crunchbase.com/organization/communications-authority-of-kenya

CSI. (2009). 14th Annual CSI Computer Crime and Security Survey: Executive Summary. New York: Computer Security Institute.

Cuman K., (2012). The Role of Internet and Social Media in International Relations. Arab revolution of 2011

Dawson, M., Omar, M., & Abramson, J. (2015). Understanding the methods behind cyber terrorism. In *Encyclopedia of Information Science and Technology, Third Edition* (pp. 1539-1549). IGI Global.

Dupuy, T. (2016). Once upon a time: re-thinking the fight against extremists. *Skeptic (Altadena, CA)*, *21*(2), 51-54.

Etaher, N., & Weir, G. (2014, June). Understanding the threat of banking malware. In *Cyberforensics 2014-International Conference on Cybercrime, Security & Digital Forensics* (pp. 73-80).

Ferguson, N., & Binks, E. (2015). Understanding radicalization and engagement in terrorism through religious conversion motifs. *Journal of Strategic Security, 8*(1), 2.

Folarin, B. (1998).Theories of Mass Communication. Ibadan, Nigeria: Sceptre Publishing

Freeman, L., Schroeder, R., & Everton, S. F. (2017). Social Media Exploitation by Covert Networks: A Case Study of ISIS. *Communications of the Association for Information Systems*, *41*(1), 5.

Galily, Y., Yarchi, M., & Tamir, I. (2015). From Munich to Boston, and from theater to social media: The evolutionary landscape of world sporting terror. *Studies in Conflict & Terrorism*, *38*(12), 998-1007.

Garcia, A. (2016). *How the Russians hacked into U.S. institutions using a fake Harvard email address.* Retrieved August 8, 2018, from Linkedin: https://www.linkedin.com/pulse/how-russians-hacked-us-institutions-using-fake-email-garcia-tobar

Garcia, A. (2016). *How the Russians hacked into U.S. institutions using a fake Harvard email address.* Retrieved August 8, 2018, from Linkedin: https://www.linkedin.com/pulse/how-russians-hacked-us-institutions-using-fake-email-garcia-tobar

Gerbaudo, P. (2018). *Tweets and the streets: Social media and contemporary activism*. Pluto Press.

Ghonim, W. (2012). *Revolution 2.0: The power of the people is greater than the people in power: A memoir*. houghton Mifflin harcourt.

Gudaitis, T. (2010). The Impact of Social Media on Corporate Security: What Every Company Needs to Know: Cyveillance, Inc.

Gulati, R. (2003). The threat of social engineering and your defense against it. *SANS Reading Room*.

Hagar, C. (2013). Crisis informatics: Perspectives of trust – is social media a mixed blessing? *SLIS Student Research Journal, 2*(2). Retrieved from http://scholarworks.sjsu.edu/slissrj/vol2/iss2/2

Harrald, J. R., Egan, D. M., & Jefferson, T. (2002). Web enabled disaster and crisis response: What have we learned from the September 11 th. In Proceedings of the Bled eConference (pp. 69–83). Retrieved from https:// domino.fov.uni-mb.si/ proceedings.nsf/ proceedings/ d3a6817c6cc6c4b5c1256e9f003bb2bd/ $file/harrald.pdf

Hecker M., Vanbremeersch N., De Durand M., Souchet T., 2012. Nature et conséquence des réseaux sociaux pour les forces armées. http:// www.defense.gouv.fr/ content/download/204906/ 2271215/file/EPS2012- Reseaux sociaux.pdf

Hinkley, C. (2011). *Social Media Makes Way for Social Engineering.* Retrieved May 18, 2018, from Security Week: https://www.securityweek.com/social-media-makes-way-social-engineering

Howard, P. N., & Parks, M. R. (2012). Social media and political change: Capacity, constraint, and consequence. *Journal of communication*, *62*(2), 359-362.

Hussaini, A., & Muhammed, A. (2016). Social Media and The Challenges Of National Security In Nigeria Muhammed. *NUBA Multidisciplinary Journal*, *1*(2), 78-89.

Innes, M. (2012). ‘Signal crimes’: detective work, mass media and constructing collective memory. In *Criminal Visions* (pp. 63-82). Willan.

Intelligence And National Security Alliance, (2011), Cyber Intelligence: setting the landscape for an emerging discipline, Arlington, VA.

ISO/IEC (2005). Information technology - Security techniques - Code of practice for information security management, ISO/IEC 17799:2005(E)

Jacobsson, S. (2010). Social Networks May Be Sharing Your Info with Advertisers. PC World.

Jansen, J. (2010). Strategic information disclosure and competition for an omperfictly protected innovation. The Journal of Industrial Economics, 58(2), 349-372.

Jones. G., (2011), Awlaki’s Death Hits al-Qaeda’s Social Media Strategy, RAND Corporation, Santa Monica, CA.

Kalçık, A. P. D. T., & Bayraktar, Ü. A. (2017). Terror Propaganda on Social Media: Daesh Terrorist Organisation. International Journal of Business and Social Science, 8(9), 128-137.

Kalçık, A. P. D. T., & Bayraktar, Ü. A. (2017). Terror Propaganda on Social Media: Daesh Terrorist Organisation. International Journal of Business and Social Science, 8(9), 128-137.

Kilcullen, D. (2006). Counter-insurgency redux. *Survival*, *48*(4), 111-130.

Kilcullen, D. J. (2006, September). Three pillars of counterinsurgency. In *US Government Counterinsurgency Conference* (Vol. 28).

KimGarst. (2018). *4 Instances When Social Media Fueled a Revolution.* Retrieved May 16, 2018, from Kim Garst: https://kimgarst.com/4-instances-when-social-media-fueled-a-revolution

Kimutai, J. K. (2014). Social Media and National Security Threats: A Case Study of Kenya. *Unpublished MA Thesis: University of Nairobi*.

Kimutai, J. K. (2014). *Social Media and National Security Threats: A Case Study of Kenya.* Retrieved April 3, 2018, from UONBI: erepository. uonbi.ac.ke/.../ Kimutai_Social%20Media%20And% 20National%20Securit...

Kohlmann, E. F. (2006). The real online terrorist threat. *Foreign Affairs*, 115-124.

Kothari, C. R. (2001). *Research Methodology Methods and Techniques* (2nd ed.). New Delhi, New Age International.

Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International

Krebs V.E., 2002. Mapping Media of Terrorist Cells. Connections 24(3), 43-52

Kumar, G., & Kumar, K. (2014). Network security–an updated perspective. *Systems Science & Control Engineering: An Open Access Journal*, *2*(1), 325-334.

Lara-Cabrera, R., Pardo, A. G., Benouaret, K., Faci, N., Benslimane, D., & Camacho, D. (2017). Measuring the radicalisation risk in social networks. *IEEE Access*, *5*, 10892-10900.

Leslie, D. A. (2014). Cyberlaundering: Concept & Practice. In *Legal Principles for Combatting Cyberlaundering* (pp. 55-117). Springer, Cham.

Leukfeldt, R., & Jansen, J. (2015). Cyber Criminal Networks and Money Mules: An Analysis of Low-Tech and High-Tech Fraud Attacks in the Netherlands. *International Journal of Cyber Criminology*, *9*(2), 173.

Leyden, J. (2012). *New stealthy botnet Trojan holds Facebook users hostage.* Retrieved August 8, 2018, from The Register: https:// www. theregister.co.uk/ 2012/01/18/carberp_ steals_e_cash_facebook/

Livingstone, S. (2008). Taking risky opportunities in youthful content creation: teenagers' use of social networking sites for intimacy, privacy and self-expression. *New media & society*, *10*(3), 393-411.

Lynch, M. (2002). The culture of control: Crime and social order in contemporary society. *PoLAR: Political and Legal Anthropology Review*, *25*(2), 109-112.

Lyon, D., & Trottier, D. (2013). Key features of social media surveillance. In *Internet and Surveillance* (pp. 109-125). Routledge.

Manjoo, F. (2004). A Picture is no Longer worth a Thousand Words.

Mansfield, R. (2010). UK MoD Secrets Leaked Onto The Internet. Retrieved January 25, 2010, from http://news.sky.com/skynews/Home/UK-News/Ministry-of-Defence-Staff-Have-Leaked-Secret-Information-16-TimesOnto-Social-Networking-Sites/Article/201001415535304

Molok, N. N. A., Ahmad, A., & Chang, S. (2011). Information leakage through online social networking: Opening the doorway for advanced persistence threats. *Journal of the Australian Institute of Professional Intelligence Officers*, *19*(2), 38.

Montagnese, A. (2012). Impact of social media on national security. *Centro Militare di Studi Strategici (Italy)*.

Moskos, C. "The Media and the Military in Peace and Humanitarian Operations." Special Report, Cantigny Conference Series, Robert R. McCormick Tribune Foundation, Chicago.

Mugenda, O. M., &Mugenda, A. G. (2003). Research Methods: Quantitative And Qualitative Approaches. Nairobi: Acts Press.

Nacos, B. (2016). *Mass-mediated terrorism: Mainstream and digital media in terrorism and counterterrorism*. Rowman & Littlefield.

Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

Newman, L. H. (2017). *The Biggest Cybersecurity Disasters of 2017 So Far.* Retrieved August 8, 2018, from Wired: https://www.wired.com/story/2017-biggest-hacks-so-far/

Omand, D., Bartlett, J., & Miller, C. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Paganini, P. (2013). *China hit by DDoS attack. The Internet inaccessible for hours.* Retrieved August 8, 2018, from security affairs: https://securityaffairs.co/wordpress/17327/cyber-crime/chinas-hit-ddos-attack.html

Panayiotides, N. (2015). The Islamic State and the redistribution of power in the Middle East. *International Journal on World Peace, 32*(3), 11.

Pandalai, S. (2016). *The 'Social Media' Challenge To National Security: Impact And Opportunities A Conceptual Overview.* New Delhi: Institute for Defence Studies and Analyses.

Park, N., & Lee, H. (2012). Social implications of smartphone use: Korean college students' smartphone use and psychological well-being. *Cyberpsychology, Behavior, and Social Networking*, *15*(9), 491-497.

Patton, D. U., Eschmann, R. D., & Butler, D. A. (2013). Internet banging: New trends in social media, gang violence, masculinity and hip hop. *Computers in Human Behavior*, *29*(5), A54-A59.

Paul, I. (2010). The Facebook data torrent debacle: Q&A. PCWorld.

Prentice S., Huffman E., 2008. Social Media's New Role in Emergency Management, Idaho National Laboratory, INL/CON-07-13552

PrenticeS.,HuffmanE., 2008. Social Media's New Role in Emergency Management, Idaho National Laboratory, INL/CON--07--13552

Qvortrup, L. (2006). Understanding new digital media: Medium theory or complexity theory?. European Journal of Communication, 21(3), 345-356.

Rauchfleisch, A., Artho, X., Metag, J., Post, S., & Schäfer, M. S. (2017). How journalists verify user-generated content during terrorist crises. Analyzing Twitter communication during the Brussels attacks. *Social Media+ Society*, *3*(3), 2056305117717888.

Reuter, C., Hughes, A. L., & Kaufhold, M. A. (2018). Social media in crisis management: An evaluation and analysis of crisis informatics research. *International Journal of Human–Computer Interaction*, *34*(4), 280-294.

Rollins J., (2011), Al Qaeda and Affiliates: Historical Perspective, Global Presence, and Implications for U.S. Policy, Congressional Research Service, Washington, DC.

Ronfeldt, D., & Arquilla, J. (2001). Networks, netwars and the fight for the future. First Monday, 6(10).

Russell, J. (2011). *Japanese government hit by Chinese Trojan horse attack.* Retrieved August 8, 2018, from henextweb: https://thenextweb.com/asia/2011/10/25/japanese-government-hit-by-chinese-trojan-horse-attack/

Scherer, M. (2011, May 30). Can They Win, One Tweet at a Time? , Time. State of California, Office of the State Chief Information Officer

Shirky, C. (2011). The political power of social media: Technology, the public sphere, and political change. *Foreign affairs*, 28-41.

Silverstein, B. (1987). Toward a science of propaganda. *Political Psychology*, 49-59.

Snow, N(2008). Routledge Handbook of Public Diplomacy. p. 338

Spaziante, L. (2017). The logic of sensorial effectiveness. Amateur videos, media witnessing, global crisis news. *Versus*, *46*(1), 17-40.

Statista. (2018). *Number of monthly active Twitter users worldwide from 1st quarter 2010 to 4th quarter 2017 (in millions).* Retrieved April 17, 2018, from Statista: https://www.statista.com/statistics/282087/number-of-monthly-active-twitter-users/

Surette, R. (2014). *Media, crime, and criminal justice*. Nelson Education.

Sutton, J.N., Spiro E., Butts C., Fitzhugh S., Johnson B., Greczek M., 2013. Tweeting the Spill: Online Informal Communications, Social Media, and Conversational Microstructures during the Deepwater Horizon Oilspill. International Journal of Information Systems for Crisis Response and Management 5-1: 58– 76

Sykora, M. D., Jackson, T. W., O'Brien, A., & Elayan, S. (2013). National security and social media monitoring: A presentation of the emotive and related systems. In *Intelligence and Security Informatics Conference (EISIC), 2013 European* (pp. 172-175). IEEE.

Tapscott, D. (2009). *Grown up digital* (Vol. 361). New York: McGraw Hill.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). *Digital crime and digital terrorism*. Prentice Hall Press.

Thompson, R. L. (2011). Radicalization and the use of social media. *Journal of strategic security*, *4*(4),9.

Thorsteinsson, G., Page, T., & Niculescu, A. (2010). Using virtual reality for developing design communication. *Studies in Informatics and Control*, *19*(1), 93-106.

Trottier, D. (2012). Policing social media. *Canadian Review of Sociology/Revue canadienne de sociologie*, *49*(4), 411-425.

Tsesis, A. (2017). Social Media Accountability for Terrorist Propaganda. *Fordham L. Rev.*, *86*, 605.

UN Counter-Terrorism Implementation Task Force, (2011), Use of the Internet to Counter the Appeal of Extremist Violence, Conference Summary, Riyadh.

Uzuegbunam, C. E. (2013). Social responsibility theory: a contemporary review. A postgraduate Seminar paper presented to the Department of Mass Communication, Faculty of Social Sciences, Nnamdi Azikiwe University Nigeria

Van Niekerk, B., & Maharaj, M. (2013). Social media and information conflict. *International Journal of Communication*, *7*, 23.

Vuori, V., & Väisänen, J. (2009, November). The use of social media in gathering and sharing competitive intelligence. In *9th Internafional Conference on Electronic Business*.

Waldman, S., & Verga, S. (2016). *Countering violent extremism on social media*. Retrieved August 25, 2018, from Defence Research and Development Canada : http://cradpdf.drdc-rddc.gc.ca/PDFS/unc262/p805091_A1b.pdf

Wanner, G. (2011). Risks of social media to organizations: Oaks publishers UK. P 64

White, E. (2018). *Taiwan hit by jump in cyber attacks from China.* Retrieved August 8, 2018, from Financial Times: https://www.ft.com/content/8e5b26c0-75c5-11e8-a8c4-408cfba4327c

Wolfsfeld, G., (2004), Media and the path to peace, Cambridge, Cambridge University Press.

Wood, G. (2015). What ISIS really wants. *The Atlantic*, *315*(2), 78-94.

Wybo, J. L., Fogelman-Soulié, F., Gouttas, C., Freyssinet, É., & Lions, P. (2015). Impact of social media in security and crisis management: a review. *International Journal of Emergency Management*, *11*(2), 105-128.

Yan, G., Chen, G., Eidenbenz, S., & Li, N. (2011, March). Malware propagation in online social networks: nature, dynamics, and defense implications. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security* (pp. 196-206). ACM.

Appendices

Appendix I: Introduction Letter

The Management,

Communication Authority of Kenya,

PO BOX 14448-00800

Nairobi, Kenya

Dear Sir/Madam,

RE: DATA COLLECTION REQUEST

I am a **student pursuing a Masters of Arts in International Conflict Management degree, Institute Of Diplomacy And International Studies at the University of Nairobi.** As part of the requirements, I am undertaking a research on "**The Impacts of Social Media on National Security of Kenya**". Your organisation was deemed the best in providing insights the required data for this study. In this regard, I am kindly requesting for permission to conduct my study in your organisation. This is an academic research and confidentiality is emphasized. Kindly accept my request. Thank you in advance

Yours Sincerely,

Dorcus Phanice Olasya

Appendix ii: Questionnaire

Please tick the box that matches your answer to the questions and give the answers in the spaces provided as appropriate. The information you provide will be treated with utmost confidentiality.

SECTION A: BASIC DEMOGRAPHIC DATA

1. Gender

Male ( )   Female ( )

2. Age

Below 20 Years ( )   20-30 Years ( )   31-40 Years ( ) 41-50 years ( )   Over 50 Years ( )

3. Highest Level of Education

Certificate [ ]   Diploma [ ]   Undergraduate [ ]   Post Graduate [ ]

4. In which department do you work?

Communication Infrastructure [ ]

Operations [ ]

Regulation and Access [ ]

Legal and Enforcement [ ]

6. How long have you worked in this organisation?

5 years or less ( )   5-10 years ( )   10 years and above ( )

THREATS OF SOCIAL MEDIA TO NATIONAL SECURITY

7. Can you consider social media a threat to national security?

Yes [ ]   No [ ]

8. Do you agree that social media are used by terrorist organizations as tools for ideological radicalization, recruitment, communication and training of its members?

Yes [ ]   No [ ]

b) If yes, to what extent do you agree that terrorists use social media as a tool for ideological radicalization, recruitment, communication and training? Use **1- Strongly agree 2- Agree 3- Undecided, 4- Disagree, 5 - Strongly disagree**

Communication	1	2	3	4	5
Ideological radicalization					
Recruitment					
Training					
Threats of violence					

9. How do you rate the current state of Kenya's national security with regard to threats from social media? Excellent [ ] Above Average [ ] Average [ ] Below Average [ ] Extremely Poor [ ]

10. To what extent does the following insecurity in Kenya been contributed by social media? Use a scale of 1 to 5 where **1 = Not at all, 2-Low extent, 3-neutral, 4-Great Extent, and 5 = Very Great extent**

Forms of insecurity	1	2	3	4	5
Terrorism attacks					
Hate speech					
Information warfare					
Tribal clashes					
Cattle rustling					
Poaching					

11. Kindly give your level of agreement the following statements regarding use of social media by criminal groups and organisations. Use a scale of 1 to 5 where **1 = to strongly disagree and 5 = strongly agree**.

Statement	**1**	**2**	**3**	**4**	**5**
Criminal organisations use social media to spread viruses					
Criminal organisations use social media to smuggle drugs	C				
Criminal organisations use social media to facilitate human trafficking					
Criminal organisations use social media to facilitate money laundering					
Criminal organisations use social media to spread and promote pornography.					

12. Kindly give your level of agreement the following statements regarding use of social media by community criminal groups such as Mombasa Republican Council (MRC), Mungiki among others. Use a scale of 1 to 5 where **1 = Not at all, 2-Low extent, 3-neutral, 4-Great Extent, and 5 = Very Great extent**

Statement	**1**	**2**	**3**	**4**	**5**
Community criminal organisations use social media to recruit new members					
Community criminal organisations use social media for communication purposes.					
Community criminal organisations use social media to spread propaganda					
Community criminal organisations use social media to radicalize youths.					
Criminal organisations use social media to spread and promote pornography.					

13. How frequent have there been cybercrime incidences that impact on the national security?

Not at all { } Slight Frequency { } Somewhat Common { } Common Very Common { }

<u>THE USE OF SOCIAL MEDIA TO PREVENT, LIMIT OR REMOVE THREATS TO NATIONAL SECURITY.</u>

14. In your opinion, do government security agencies use social media platforms to enhance national security?

Yes { } No { }

b) If Yes, kindly elaborate

………

15. Are there officers whose job includes spending time on social media sites to monitor the content shared and any security threat that spreads around?

Yes [ ] No [ ]

b) If Yes, kindly elaborate

………

16. Kindly give your level of agreement the following statements regarding use of social media by security agencies to curb and minimize threats to national security. Use a scale of 1 to 5 where **1 = to strongly disagree and 5 = strongly agree**.

Statement	1	2	3	4	5
Security agencies mostly use social media to counter propaganda					
Security agencies mostly use social media to promote public diplomacy					
Security agencies mostly use social media for open source intelligence					
Security agencies mostly use social media to communicate with the public.					

STRATEGIES USED TO CURB AND MINIMIZE THE NEGATIVE EFFECTS OF SOCIAL MEDIA ON THE NATIONAL SECURITY

17. What strategies have been put in place to curb and minimize the social media threats to national security?

....
....

18. Do you have tools that help in the analysis of social media threats to national security?

Yes [ ]   No [ ]

b) If yes, which ones?

……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………

19. Give suggestions of how people can protect themselves against offensive use of social media and improve on the security situation in the country

……………………………………………………………………………………………
……………………………………………………………………………………………

THANK YOU FOR PARTICIPATING

Appendix II: interview guide for the national cohesion and integration commission (ncic) official, directorate of criminal investigation official, and an official from the national intelligence service.

1. Gender of the respondent

2. Age bracket

3. Level of education

4. For how many years have you served in your current position?

5. What is your perception on the effect of social media on national security?

6. Can you consider social media a threat to national security?

7. Give your views on the use of social media by terrorist organisations. In your opinion, does this pose a threat to national security?

8. In your opinion, for what purpose do terrorist organisations mostly use social media platforms?

9. Give us your opinion on the current state of Kenya's national security with regard to threats of social media?

10. Give your views on the extent to which social media use has facilitated terrorism attacks, hate speech, information warfare, cyber-attacks, spread of malware, and tribal clashes

11. Dou think social media platforms are widely used in Kenya to spread viruses, smuggle drugs, facilitate human trafficking, and to facilitate money laundering? Kindly elaborate

12. In your own views, please tell us the various ways the community criminal gangs use social media platforms. To what extent does this impact on national security?

13. Do you think security agencies in the country are utilizing social media networks to effectively to remove threats to national security? Kindly elaborate

14. What are the main strategies that have been put in place to curb and minimize the social media threats to national security?

15. Do you think the government security agencies have won the fight against the misuse of social media platforms?

16. Kindly give us your views on the use of social media by security agencies to counter propaganda, to promote public diplomacy, for open source intelligence, and to communicate with the public.

17. What areas do you think should still be improved to minimize the threats of social media to national security?

THANK YOU FOR PARTICIPATING

Appendix III: Questionnaire for the General Public

Please tick the box that matches your answer to the questions and give the answers in the spaces provided as appropriate. The information you provide will be treated with utmost confidentiality.

1. Gender

Male ( ) Female ( )

2. Age

Below 20 Years ( ) 20-30 Years ( ) 31-40 Years ( ) 41-50 years ( ) Over 50 Years ( )

3. Highest Level of Education

Primary [ ] Secondary Level [ ] Certificate [ ] Diploma [ ] Undergraduate [ ] Post Graduate [ ]

4. Can you consider social media a threat to national security?

Yes [ ] No [ ]

5. How do you rate the current state of Kenya's national security with regard to threats from social media? Excellent [ ] Above Average [ ] Average [ ] Below Average [ ] Extremely Poor [ ]

6. Do you agree that social media platforms are used by terrorist organizations and criminals as tools for ideological radicalization, hate speech, recruitment, money laundering, cyber-crime, tribalism, communication and training of its members, spread of viruses, smuggling, drug trafficking, and poaching?

Yes [ ] No [ ]

b) If yes, to what extent do you agree to each of each of the following uses of social media by criminal organisations and terrorists? Use 1- No extent, 2- small extent, 3- Moderate extent, 4- Large extent, 5 – Very large extent

Communication	1	2	3	4	5
Hate speech					
Recruitment & Training					
Money laundering					
Cyber crime					
Tribalism					
Spread of malware					
Drug trafficking					
Ideological radicalization					
Poaching					

7. In your opinion, do government security agencies use social media platforms to enhance national security?

Yes { } No { }

b) If yes, kindly elaborate

…………………………………………………………………………………………………

8. Do you think the government security agencies have won the fight against the misuse of social media platforms?

Yes { } No { }

THANK YOU FOR PARTICIPATING